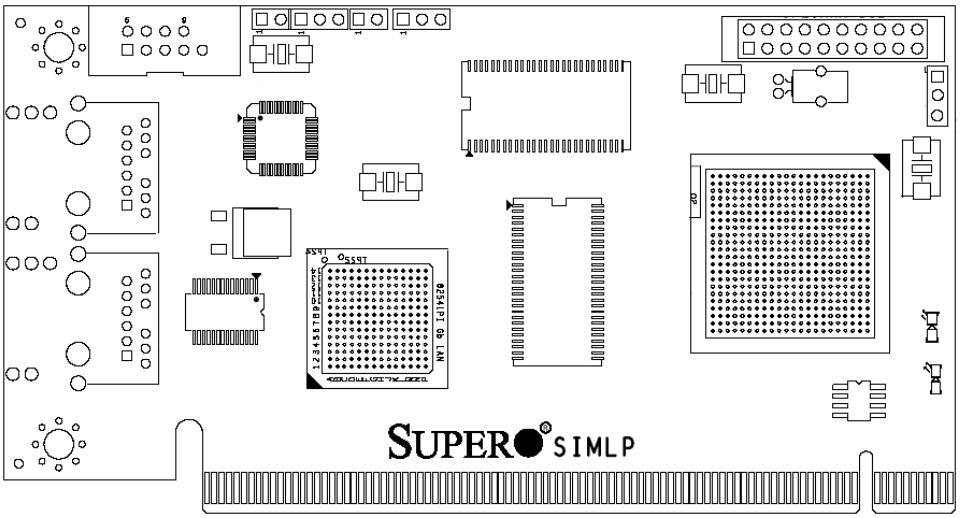
SUPERO®

SUPERO® AOC-SIMLP-B

SUPERO® AOC-SIMLP-B+

SUPERO® AOC-SIMLP-3

SUPERO® AOC-SIMLP-3+



USER'S GUIDE

Rev. 1.0

The information in this User's Guide has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates.

Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

SUPERMICRO COMPUTER reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

IN NO EVENT WILL SUPERMICRO COMPUTER BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, THE VENDOR SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision: Rev. 1.0

Release Date: July 21, 2006

Unless you request and receive written permission from SUPER MICRO COMPUTER, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2006 by SUPER MICRO COMPUTER, INC.
All rights reserved.

Printed in the United States of America

Table of Contents

Chapter I: Introduction 1-4

1.1 Overview 1-4

1.2 IPMI Version 2.0 1-5

1.3 Product Features 1-6

1.4 Checklist 1-6

1.5 An important Note to the User 1-6

1.6 Contacting Supermicro 1-7

Chapter 2: Technical Specifications and Software Installation 2-1

2.1 AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ Card Layout and Jumper ..... Locations 2-1

2.2 Block Diagram 2-3

2.3 Safety Guidelines 2-4

Chapter 3: Software Application and Usage 3-1

3.1. Home Page 3-3

3.2. Functions Listed On the Home Page 3-5

3.2.1. Remote Control 3-5

3.2.2. Virtual Media 3-7

3.2.3. System Health 3-11

3.2.4. User Management 3-17

3.2.5. KVM Settings 3-21

3.2.6. Device Settings 3-25

3.2.7. Maintenance 3-38

Chapter 1 Introduction

This manual is written for system integrators, PC technicians and knowledgeable PC users who intend to integrate Supermicro's unique IPMI 2.0 Management functionality with the capability of KVM-over-LAN into their systems. It provides detailed information for the application and use of the AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ that supports remote access for system monitoring, diagnosis and management. With the most advanced technologies built-in, the AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ offers a complete, efficient, and cost effective remote server management.

1.1 Overview

The AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ is a highly efficient, highly compatible and easy-to-use IPMI card that allows the user to take advantage of BMC, a baseboard management controller installed on a server motherboard and the IPMIView, an IPMI-compliant management application software loaded in a PC, to provide serial links between the main processor and other system components, allowing for network interfacing via remote access. With an independent Peppercon's KIRA100 processor built-in, the AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ provides the user a solution to ease the complex and expensive systems, allowing an administrator to access, monitor, diagnose and manage network interfacing anywhere, anytime.

1.2 IPMI Version 2.0

The AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ supports the functionality of IPMI Version 2.0. The key features include the following:

- Supports IPMI over LAN
- Supports Serial over LAN
- Supports KVM over LAN (*AOC-SIMLP-B+, AOC-SIMLP-3+ only)
- Supports Virtual Media over LAN
- Supports LAN Alerting-SNMP Trap
- Supports Event Log
- Offers OS (Operating System) Independency
- Provides remote Hardware Health Monitoring via IPMI. Key features include the following:
    - Temperature sensoring,
    - Fan speed monitoring
    - Voltage monitoring
    - Power status monitoring, chassis intrusion monitoring
    - Remote power control to power-on, power-off or reboot a system

- Remote access to text-based, graphic-based system information, including BIOS configurations and OS operation information (KVM)
- Remote management of utility/software applications

- Provides Network Management Security via remote access/console redirection. Key features include:
  - User authentication enhancement
  - Encryption support enhancement, allowing for password configuration security to protect sensitive data transferring via Serial over LAN

1.3. Product Features

(a) The AOC-SIMLP-B/SIMLP-B+ Series: (IPMI 2.0 with a Dedicated LAN)

- Low profile Form Factor (5.1" W x 2.7" H) (129.3 mm W x 68.8 mm H)
- Supports 2U systems and above
- Supports IPMI over LAN

(b) The AOC-SIMLP-3/SIMLP-3+* Series: (IPMI 2.0 with a Dedicated LAN and the Intel 82541PI GLAN Controller)

- Low profile Form Factor (5.1" W x 2.7" H) (129.3 mm W x 68.8 mm H)
- Supports 2U systems and above (*AOC-SIMLP-3/AOC-SIMLP-3+ only)
- Supports IPMI over LAN
- Intel's 82541 PI Gigabit LAN Controller (with 3rd data LAN support)
- The AOC-SIMLP-3+ supports KVM

(c) Features Supported by Individual Models

Features	Dedicated LAN for IPMI	Intel 82541 PI for Data Transmission	KVM-over-LAN
SIMLP-B	Yes	-----	-----
SIMLP-B+	Yes	-----	Yes
SIMLP-3	Yes	Yes	-----
SIMLP-3+	Yes	Yes	Yes

1.4 CheckList

If your shipping package came with missing or damaged parts, please contact Supermicro's Tech. Support. Please refer to the following checklist when contacting us.

i. AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+:

ii. Brackets: One full-size bracket, one low-profile bracket and two screws,

iii. CDR-SIMIPMI: One Installation CD

iv. White Box with Correct Barcode Label (showing AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+).

1.5 An Important Note to the User

The drawings and pictures shown in this manual were based on the latest PCB Revision available at the time of publishing of the manual. The AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ card you've received may or may not look exactly the same as the graphics shown in the manual.

1.6 Contacting Supermicro

Headquarters

Address: SuperMicro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.
Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)
Web Site: www.supermicro.com

Europe

Address: SuperMicro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands
Tel: +31 (0) 73-6400390
Fax: +31 (0) 73-6416525
Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)

Asia-Pacific

Address: SuperMicro, Taiwan
4F, No. 232-1 Liancheng Road
Chung-Ho 235, Taipei Hsien, Taiwan, R.O.C.
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3991
Web Site: www.supermicro.com.tw

Technical Support:
Email: support@supermicro.com.tw

Notes

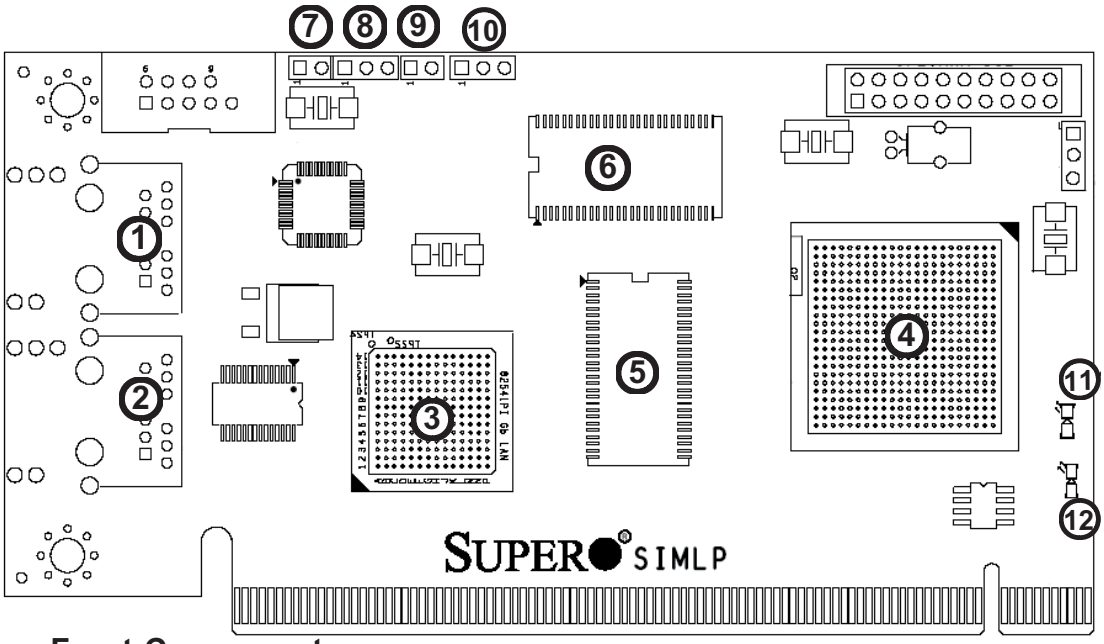
Chapter 2

Technical Specifications and Software Installation

2.1 AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ Card Layout and Jumper Locations

SUPER® AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ Card Layout and Jumper Locations

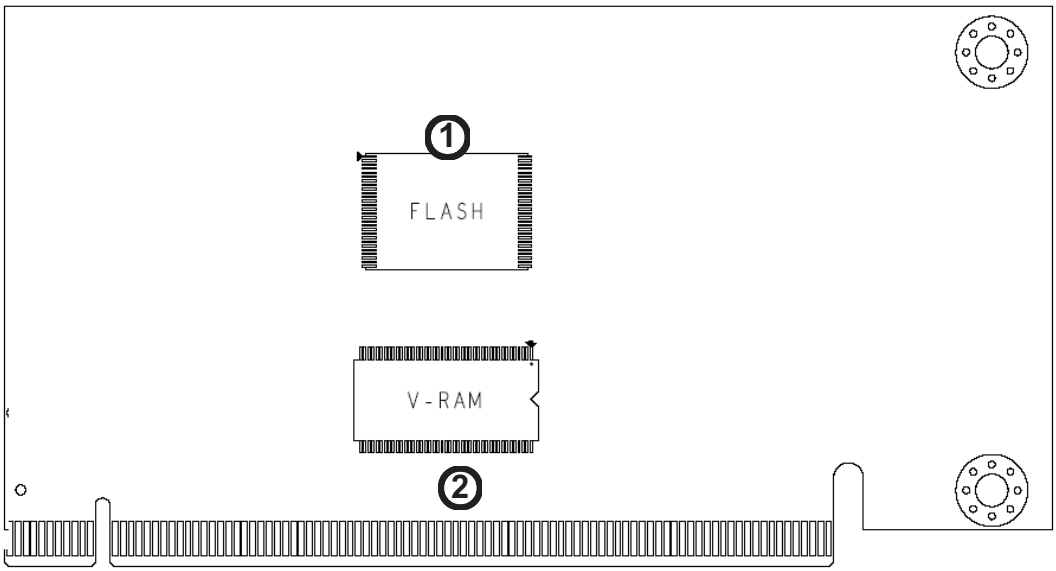
Front View



Front Components

1. LAN Port 1 (JLAN1) for IPMI/Keyboard/Video/Mouse over IP
2. LAN Port 2 (JLAN2) for 3rd Data via Intel's 82541PI Controller
3. Intel's 82541PI GLAN Controller
4. Peppercon's KIRA 100 Processor
5/6. SDRAM (128Mb/133MHz)
7. JP5: LAN Port1 Activity LED Jumper
8. JP7: JLAN 2 Control Jumper
9. JP6: GLAN Port2 Activity LED Jumper
10. JP1: JLAN1 Control Jumper
11. D3: Power-on LED
12. D4: Heart-beat (Activity) LED

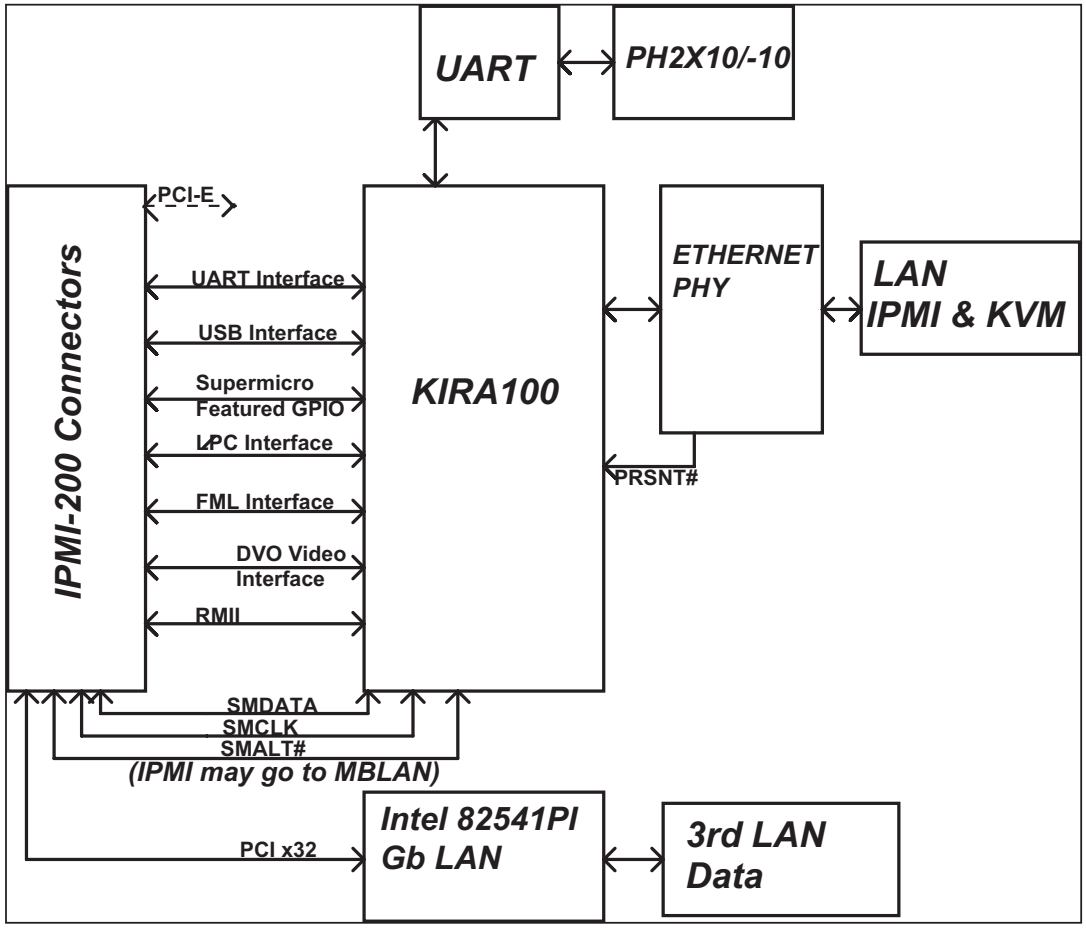
Rear View



Rear Side Components

1. Flash DRAM (64Mb/133MHz)
2. VRAM (64Mb/166MHz)

2.2 Block Diagram



2.3 Safety Guidelines

To avoid personal injury and property damage, please carefully follow all the safety steps listed below when accessing your system or handling the components:

ESD Safety Guidelines

Electric Static Discharge (ESD) can damage electronic components. To prevent damage to your system. it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing a component from the antistatic bag.
- Handle the IPMI card by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules, avoid touching their pins.
- Put the card and peripherals back into their antistatic bags when not in use.

General Safety Guidelines

- Always disconnect power cables before installing or removing any components from the computer.
- Use only the correct type of bracket for the chassis. Please use a full-height bracket for a 1U, 3U, 4U, Tower, or a Pedestal system. Use a low-profile bracket for a 2U or some of the proprietary chassis. Make sure to secure the bracket in the host system cabinet. (*Note: When used in a 1U system, the full-height bracket is mounted into the riser card.)
- Disconnect the power cable before removing the data cable from the riser card.
- Make sure that the IPMI card is securely seated in the PCI slot to prevent damage to the system due to power shortage.

Chapter 3

Software Application and Usage

With an independent I/O processor embedded in Peppercon's KIRA 100 chip, the AOC-SIMLP-B/SIMLP-B+/SIMLP-3/SIMLP-3+ Add-On Card allows the user to access, monitor, manage and interface with systems that are in remote locations via LAN. The necessary drivers are all included on the Supermicro bootable CDs that came with your card. This section provides information on network interfacing via remote access.

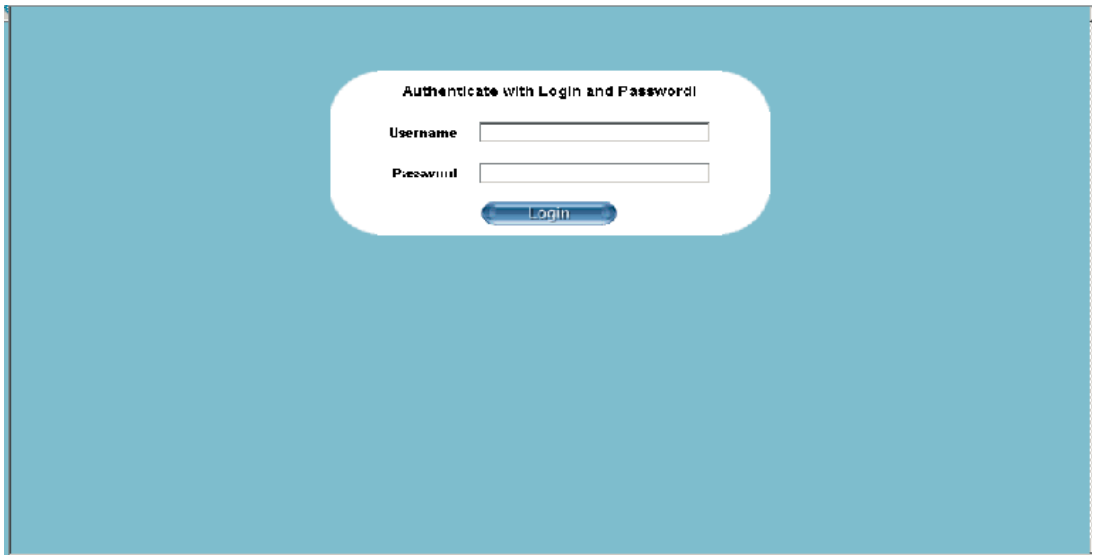
Network Connection

1. Type the IP address of each server that you want to connect in the address bar in your browser.

2. Once the connection is made, the Log In screen as shown on the next page displays.

To Log In

Once you are connected to the remote server, the following Log In screen displays.

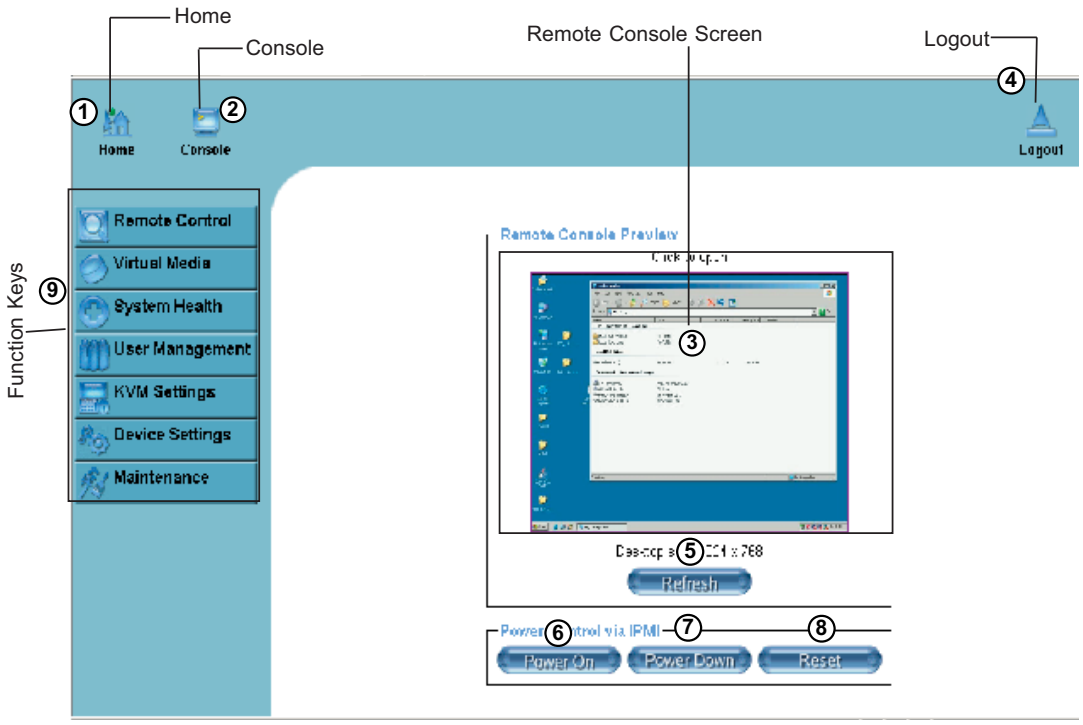


1. Type in your Username in the "Username" box.
2. Type in your Password in the "Password" box and click on "Login."

(***Note**: The default username is ADMIN. The default password is ADMIN.)

3. The Home Page will display as follows:

A. Home Page



Buttons from the Home Page

① **Home**: Click this icon to return to the Home Page.

② **Console**: Click this icon to go to Remote Console Screen.

③ **Remote Console Screen**: Displayed in the window is Remote Console Screen. Click on this window to go to Remote Console Screen.

④ **Logout**: Click on this icon to log out.

⑤ **Refresh**: Click on this icon to refresh the screen of the remote console preview.

⑥ **Power On**: Click on this icon to power on the system of the remote host.

⑦ **Power Down**: Click on this icon to power down the system of the remote host.

⑧ **Reset**: Click on this icon to reset the remote host.

Function Keys from the Home Page

⑨ Click on these function keys to use the functions as specified below.

① **1. Remote Control**: Click on this icon for remote access and management of Video Console Redirection.

② **2. Virtual Media**: Click on this icon to use virtual remote media devices.

③ **3. System Health**: Click on this icon to view and manage health monitoring for remote systems

④ **4. User Management**: Click on this icon for User Management.

⑤ **5. KVM Settings**: Click on this icon to configure keyboard, Video and mouse settings.

⑥ **6. Device Settings**: Click on this icon to configure device settings.

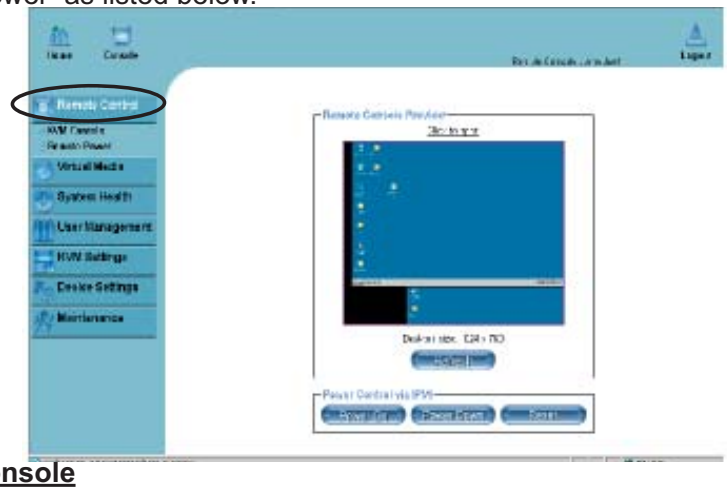
⑦ **7. Maintenance**: Click on this icon to access, diagnose and manage hardware devices

(***Note**: Please see the next page for details on the functions specified above.)

B. Functions Listed on the Home Page

3.2.1. Remote Control

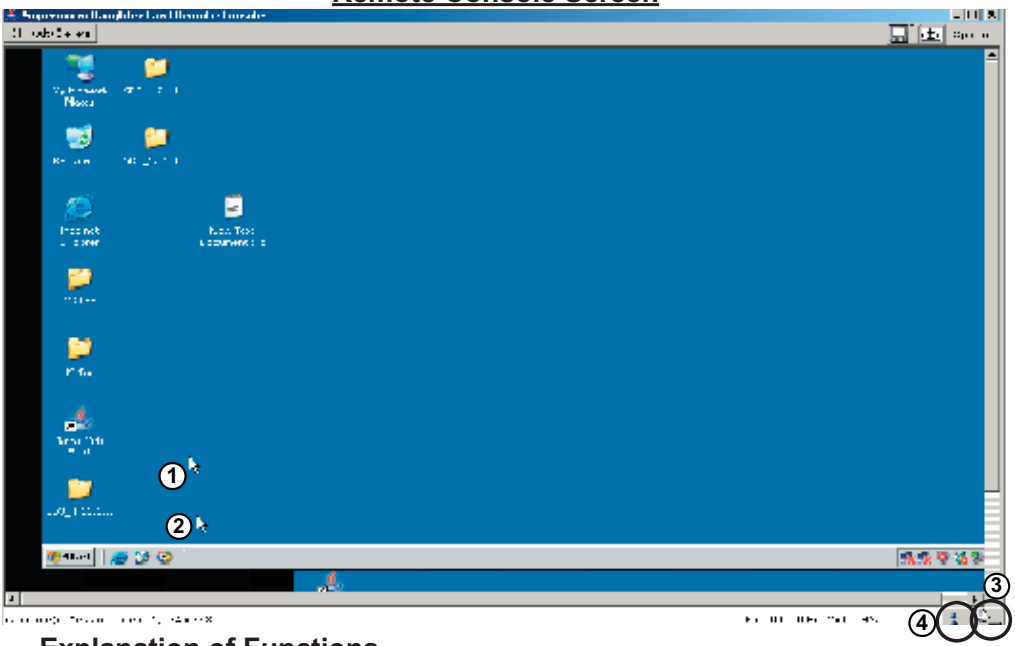
Click on the icon of Remote Control to activate its submenus-KVM Console and Remote Power as listed below.



a. KVM Console

Click on this item to configure keyboard, mouse or video settings for the remote host.

Remote Console Screen



Explanation of Functions

① In the Single/Synchronized Mouse Mode, this cursor indicates the system that is currently active. For the Double Mouse mode, this is the cursor for the remote host.

② This second mouse cursor only appears in the Double Mouse Mode. This cursor represents the local mouse.

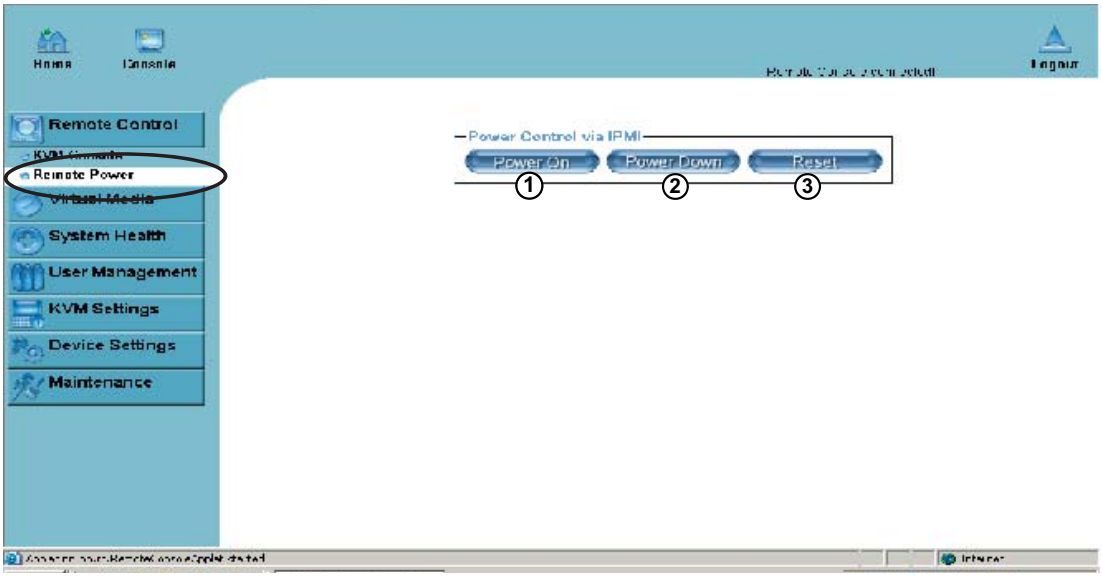
③ This icon indicates the availability of Keyboard and Mouse.

④ This icon indicates the number of networks (users) that are connected via Console Redirection. (The number of figure icons indicates the number of users connected.)

b. Remote Power

Click on this item to configure the power settings for Remote Console as shown below.

Remote Power Screen



Explanation of Functions

①

Power On: Click on this icon to power on the remote host.

②

Power Down: Click on this icon to power down the remote host.

③

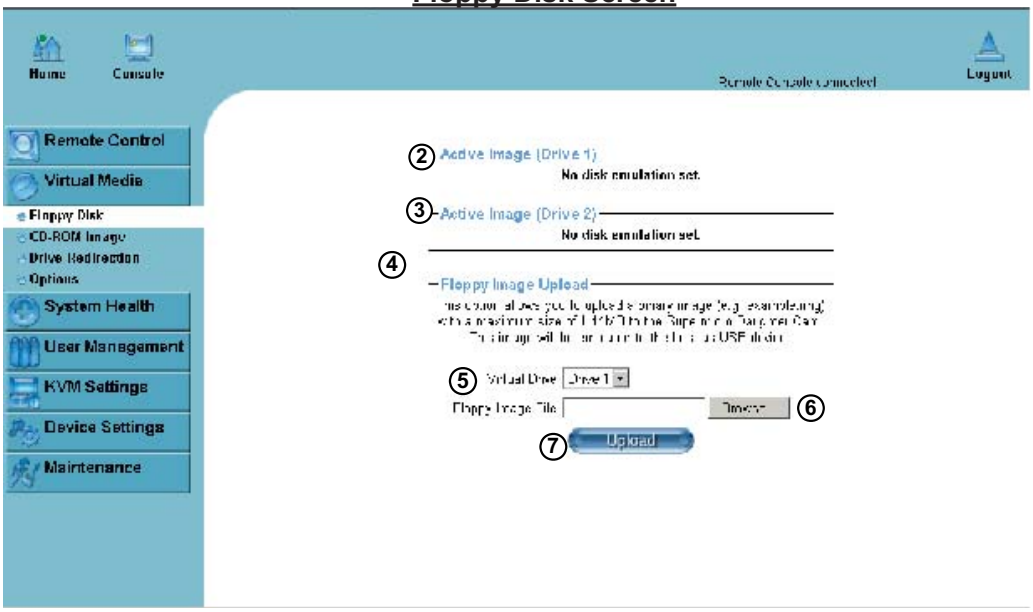
Reset: Click on this icon to reset the remote host.

3.2.2. Virtual Media

Click on the Virtual Media icon on the Home Page to activate its submenus-Floppy Disk, CD-ROM, Drive Redirection and Options as listed below.

a. Floppy disk

Floppy Disk Screen



Explanation of Functions

①

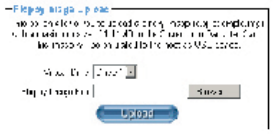
Floppy Disk: Click on this function key to upload the data stored in the local floppy disk image to the remote host.

②

Active Image (Drive1): This window displays the data that has been uploaded to Drive 1 of the remote host.

③

Active Image (Drive2): This window displays the data that has been uploaded to Drive 2 of the remote host.

④ 

Floppy Image Upload: This option allows the user to upload the floppy image as "floppy" located in the remote host. The floppy image uploaded shall be in the binary format with a maximum size of 1.44MB. It will be loaded to the Supermicro SIMLP card and will be emulated to the host as a USB device.

⑤

Virtual Drive: Select a drive in the remote host as a destination drive for you to upload your image data.

⑥

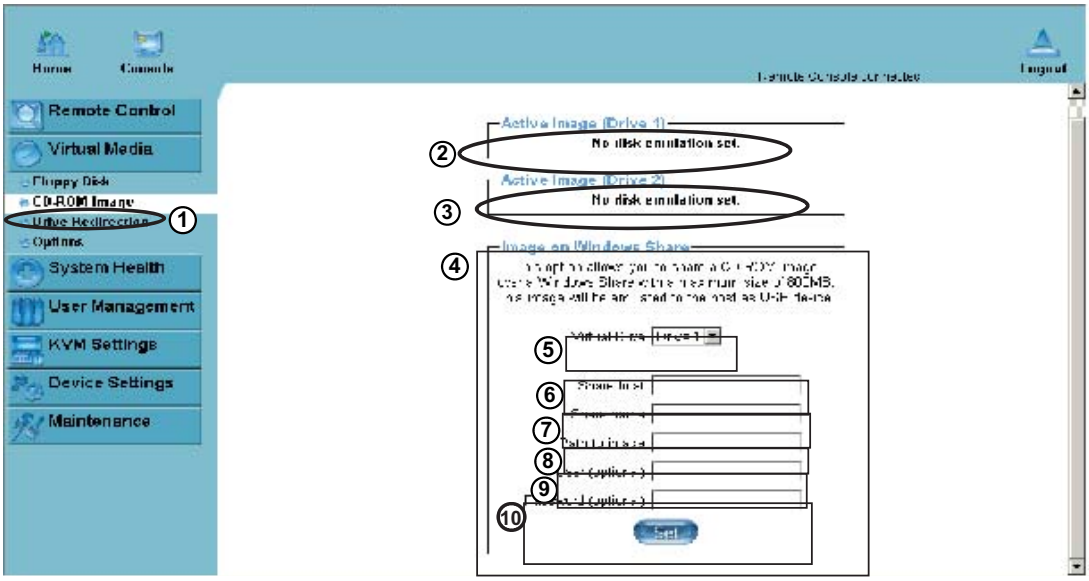
Floppy Image File: Click on "Browse" to preview and select the files that you wish to upload to the host drive selected.

⑦

Upload: Once the correct file name appears in the box, click Upload to upload the floppy image to the drive specified in the remote host.

b. CD-ROM Image

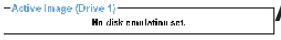
CD-ROM Image Screen



Explanation of Functions

①

CD-ROM image: Click on this function key to share data stored in your local CD-ROM drive with other users in the remote host through the Windows Share application via USB.

② 

Active Image (Drive1): This window displays the file name of the data currently active in host Drive 1.

③

Active Image (Drive2): This window displays the file name of the data currently active in host Drive 2.

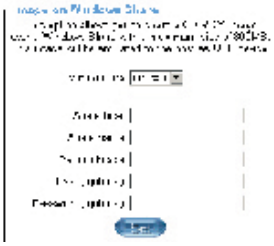
④ 

Image on Windows Share: This option allows the user to configure Windows Share settings. It allows you to decide how you want to share the data stored in your local CD-ROM with users in the remote host.

⑤

Virtual Drive: Specify the drive that you want to share your data with in the remote host.

⑥

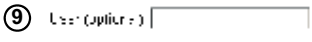
Share Host: Key in the IP Address or the name of the system you wish to share data with via Windows Share.

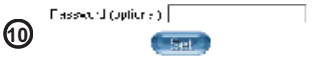
⑦

Share Name: Key in the name of the system you wish to share data with in the remote host.

⑧

Path to Image: Key in the location of source files that you wish to share via Windows Share.

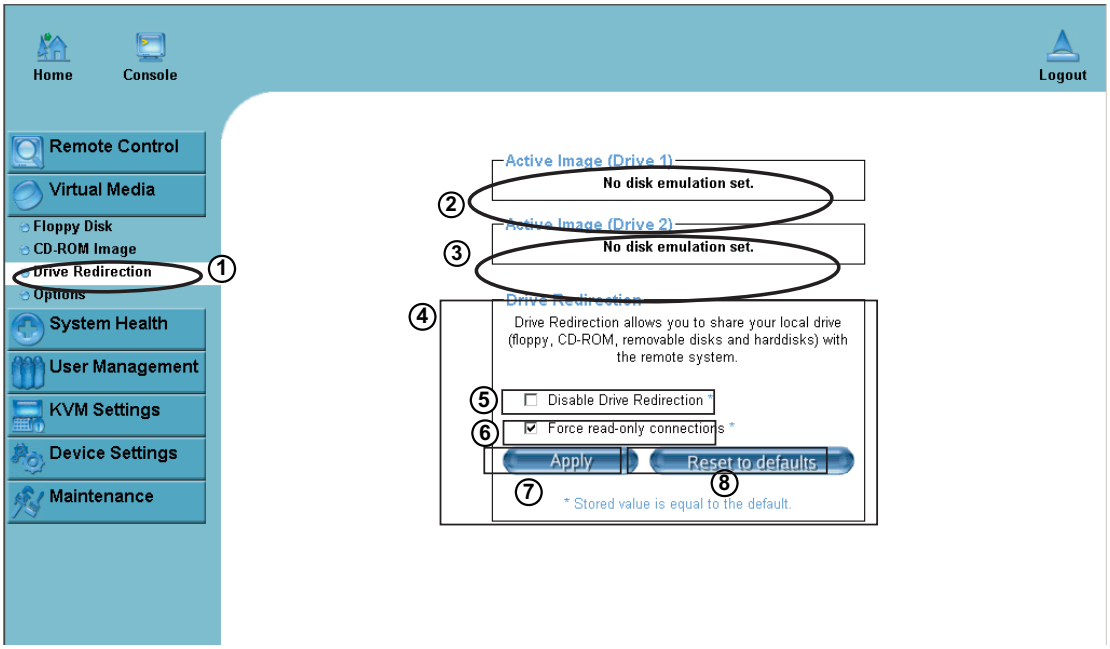
⑨ 

⑩ 

User/Password (Optional): Key in the Username and password for the person to access the data that you want to share and click "Set" to enter your selections.

c. Drive Redirection

Drive Redirection Screen



Explanation of Functions

① Drive Redirection

Drive Redirection: Click on this function key to make local drives accessible for other users via console redirection. This function allows you to share your local drives (Floppy, CD-ROM and HDDs) with users in the remote systems.

② Active Image (Drive 1) — No disk emulation set.

Active Image (Drive1): This window displays the file name of the data currently active in host Drive 1.

③ Active Image (Drive 2) — No disk emulation set.

Active Image (Drive2): This window displays the file name of the data currently active in host Drive 2.

④

Drive Redirection: Use this window to configure Drive Redirection settings.

⑤ ☐ Disable Drive Redirection *

Disable Drive Redirection: Check the box to disable Drive Redirection. Once this function is disabled, local drives will not be accessible for other users in remote host.

⑥ ☑ Force read-only connections

Force Read Only: Check this box to allow the data stored in local drives to be read in a remote system, but it cannot be overwritten to ensure data integrity and system security.

⑦ Apply

Apply: Once you've configured your settings, click "Apply" to enter your settings.

⑧ Reset to defaults

Reset Default: You can also key in your own setting values and re-set these values as "default" by clicking on this icon to reset the defaults.

d. Virtual Media Options

Virtual Media Options Screen

Explanation of Functions

①

Options: Click on this function key to activate the Virtual Media sub-menu.

②

Virtual Media Options: Use this option to disable or enable USB MASS storage in the remote host. Check this box to disable the function of Virtual Media Options to prevent data stored in a local drive from being accessed, or uploaded by the user in the remote host. The default setting is "enabled."

③

Apply: Once you've checked the box, click "Apply" to enter this value.

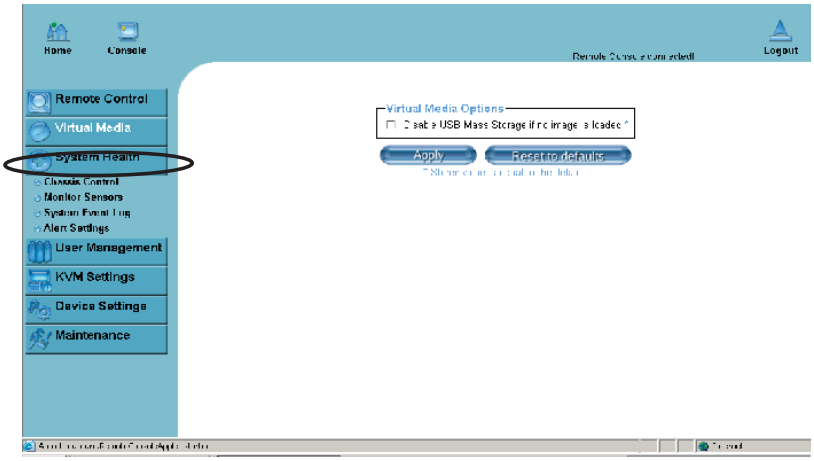
④

Reset to Defaults: If you want to set "Disabled" as the default setting for the item-Virtual Media Options, click on this icon.

3.2.3. System Health

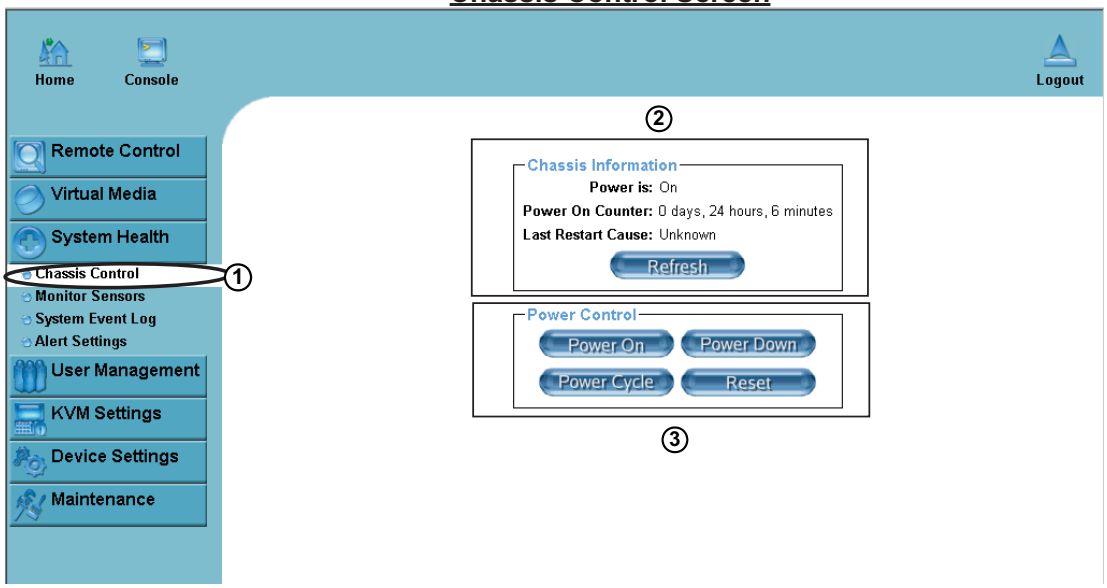
Click on the System Health icon on the Home Page to activate its submenus: Chassis Control, Monitor Sensor, System Event Log and Alert settings as listed below.

System Health Screen



a. Chassis Control

Chassis Control Screen



① **Chassis Control**

Chassis Control: Click on this function key to access Health Monitoring information on the remote chassis. The items monitored include 1. Chassis Information 2. Power Control.

② **Chassis Information:**

The following remote chassis information is included:

***Power Is**: This indicates if the system is on or off for the remote host.

***Power On Counter**: If power is on, then the counter indicates the length of time the power has been turned on.

***Last Restart Cause**: This item states the reason why the host system is restarted if the system has been turned off.

* **Refresh**: Click the Refresh button to update "Chassis Information" as shown in Window 2.

③ Power Control

The following Power Control items are included:

Refresh: Click on this icon to refresh the screen of the remote host.

Power On: Click on this icon to power on the system for the remote host.

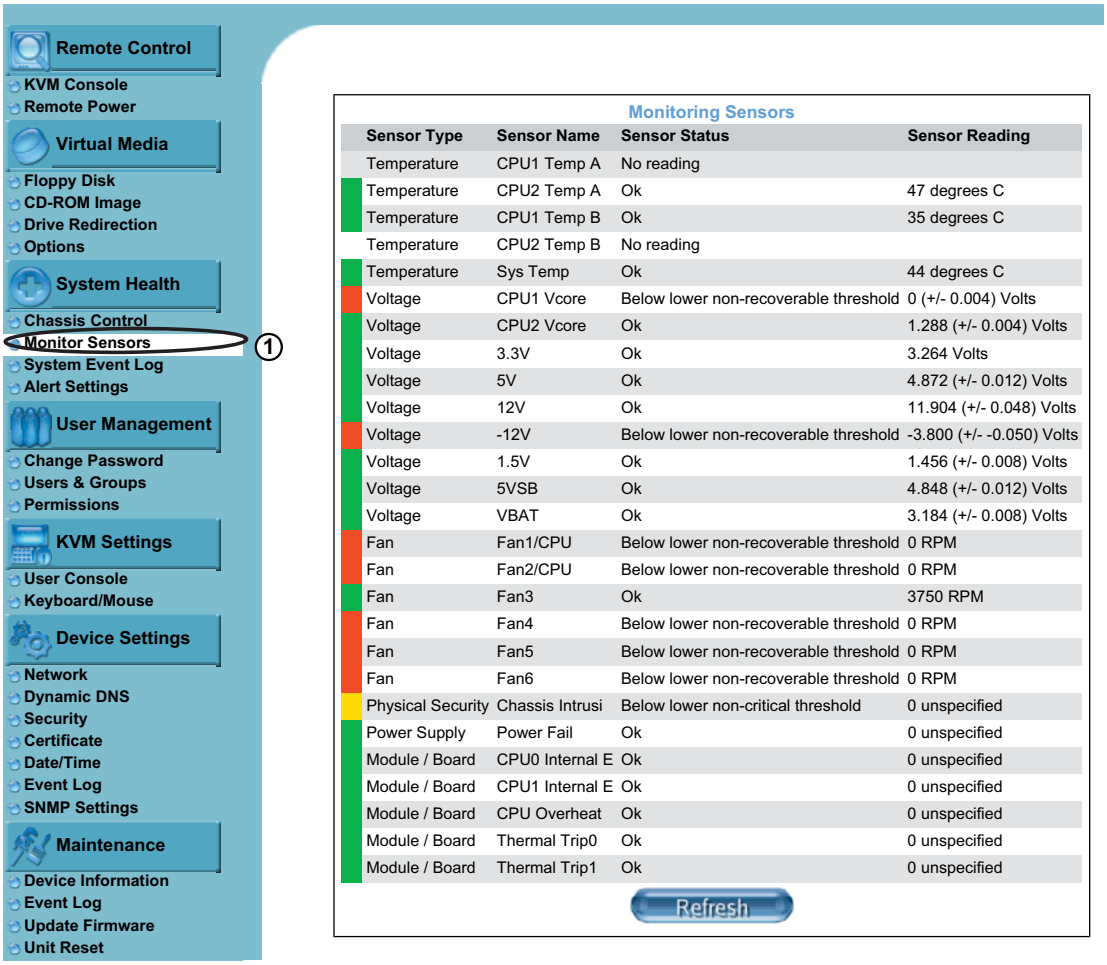
Power Down: Click on this icon to power down the system for the remote host.

Power Cycle: Click on this icon to power down the system for the remote host and turn it back on later.

Reset: Click on this icon to reset the remote console.

b. Monitor Sensors

Monitor Sensors Screen

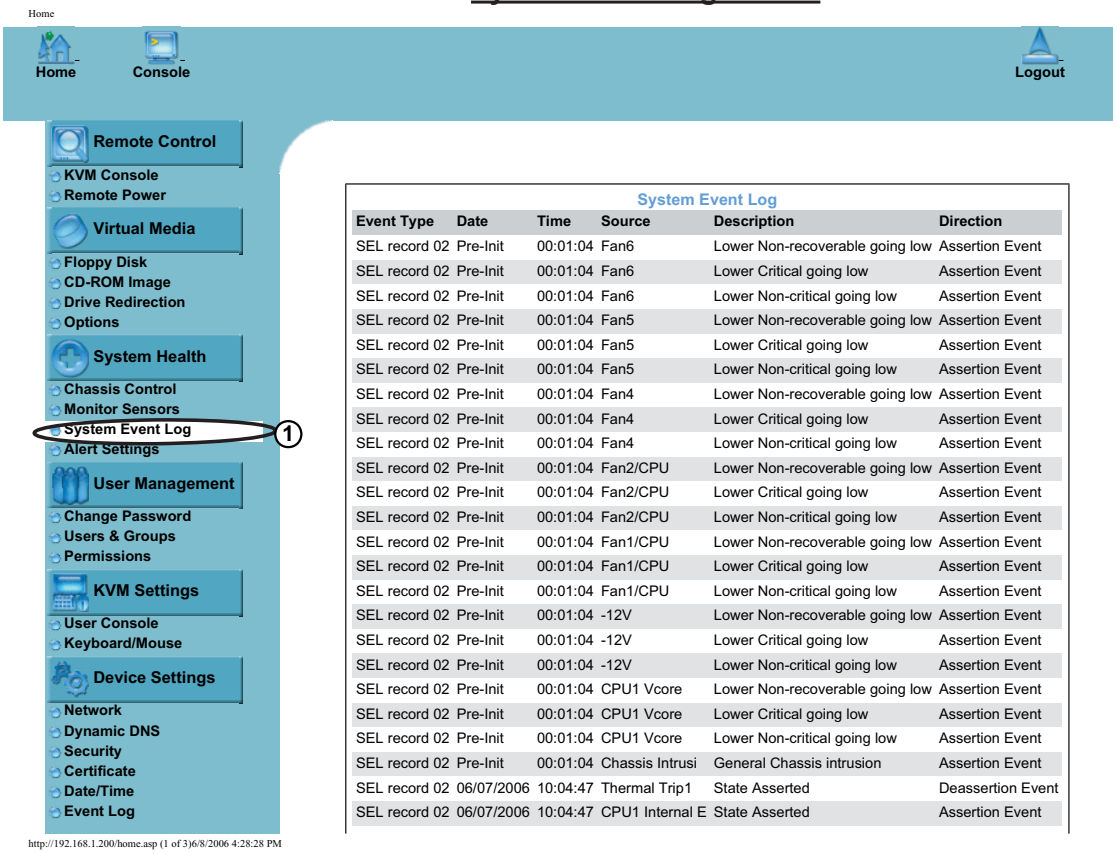

Remote Control
KVM Console
Remote Power
Virtual Media
Floppy Disk
CD-ROM Image
Drive Redirection
Options
System Health
Chassis Control
Monitor Sensors
System Event Log
Alert Settings
User Management
Change Password
Users & Groups
Permissions
KVM Settings
User Console
Keyboard/Mouse
Device Settings
Network
Dynamic DNS
Security
Certificate
Date/Time
Event Log
SNMP Settings
Maintenance
Device Information
Event Log
Update Firmware
Unit Reset
1
Monitoring Sensors
Sensor Type | Sensor Name | Sensor Status | Sensor Reading
Temperature | CPU1 Temp A | No reading
Temperature | CPU2 Temp A | Ok | 47 degrees C
Temperature | CPU1 Temp B | Ok | 35 degrees C
Temperature | CPU2 Temp B | No reading
Temperature | Sys Temp | Ok | 44 degrees C
Voltage | CPU1 Vcore | Below lower non-recoverable threshold | 0 (+/- 0.004) Volts
Voltage | CPU2 Vcore | Ok | 1.288 (+/- 0.004) Volts
Voltage | 3.3V | Ok | 3.264 Volts
Voltage | 5V | Ok | 4.872 (+/- 0.012) Volts
Voltage | 12V | Ok | 11.904 (+/- 0.048) Volts
Voltage | -12V | Below lower non-recoverable threshold | -3.800 (+/- -0.050) Volts
Voltage | 1.5V | Ok | 1.456 (+/- 0.008) Volts
Voltage | 5VSB | Ok | 4.848 (+/- 0.012) Volts
Voltage | VBAT | Ok | 3.184 (+/- 0.008) Volts
Fan | Fan1/CPU | Below lower non-recoverable threshold | 0 RPM
Fan | Fan2/CPU | Below lower non-recoverable threshold | 0 RPM
Fan | Fan3 | Ok | 3750 RPM
Fan | Fan4 | Below lower non-recoverable threshold | 0 RPM
Fan | Fan5 | Below lower non-recoverable threshold | 0 RPM
Fan | Fan6 | Below lower non-recoverable threshold | 0 RPM
Physical Security | Chassis Intrusi | Below lower non-critical threshold | 0 unspecified
Power Supply | Power Fail | Ok | 0 unspecified
Module / Board | CPU0 Internal E | Ok | 0 unspecified
Module / Board | CPU1 Internal E | Ok | 0 unspecified
Module / Board | CPU Overheat | Ok | 0 unspecified
Module / Board | Thermal Trip0 | Ok | 0 unspecified
Module / Board | Thermal Trip1 | Ok | 0 unspecified
Refresh

① **Monitoring Sensor**: Click on this function key to display the following Health Monitoring Information shown in the following table:

Health Monitoring Sensor Information on the Remote Host		
Temperature Monitoring	CPU1 Temperature (Temp A, Temp B)	Temp A: CPU1 Core1 Temperature, Temp B: CPU1 Core2 Temperature,
	CPU2 Temperature (Temp A, Temp B)	Temp A: CPU2 Core1 Temperature, Temp B: CPU2 Core2 Temperature,
	System Temperature	
Voltage Monitoring	CPU1 VCore	CPU1 Vcore: CPU1 Core Voltage
	CPU2 VCore	CPU2 Vcore: CPU2 Core Voltage
	3.3V	
	5V, 5VSB	5VSB: 5V Standby
	+12V, -12V	
	1.5V	
	VBAT	VBAT: Battery Voltage
Fan Control	Fan1/CPU Fan	
	Fan2/CPU Fan	
	Fan 3 – Fan 6	System Fans/Chassis Fans
Physical Security	Chassis Intrusion	
Module/Board CPU0 Internal E.		
Module/Board CPU1 Internal E.		
Module/Board CPU Overheat		When the CPU temperature exceeds this preset temperature, the overheat LED or alert will be triggered, the CPUs will slow down, the CPU fans will be in the full speed mode.
Module/Board Thermal Trip		When the system temperature exceeds this preset temperature, the overheat LED or alert will be triggered, and the cooling fans will be in the full speed mode to prevent system overheat.

c. System Event Log

System Event Log Screen



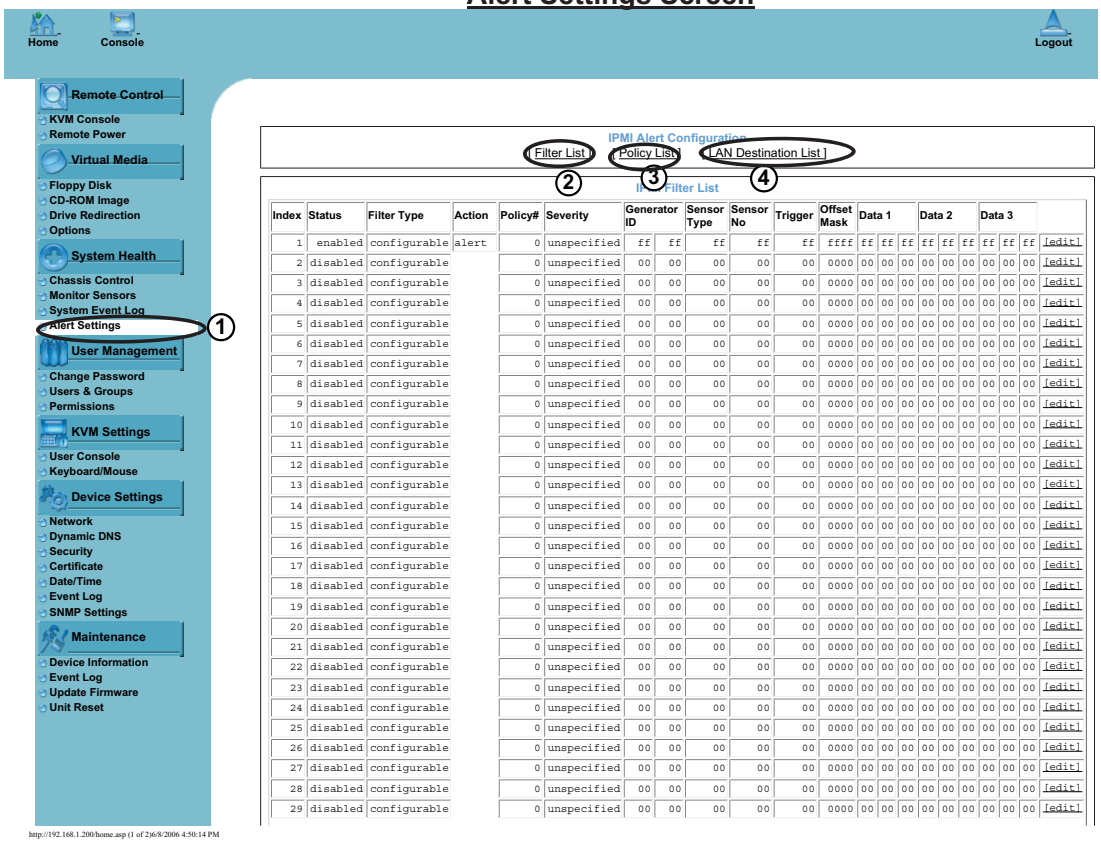
System Event Log

Event Type	Date	Time	Source	Description	Direction
SEL record 02	Pre-Init	00:01:04	Fan6	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan6	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan6	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan5	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan5	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan5	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan4	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan4	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan4	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan2/CPU	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan2/CPU	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan2/CPU	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan1/CPU	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan1/CPU	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Fan1/CPU	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	-12V	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	-12V	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	-12V	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	CPU1 Vcore	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	CPU1 Vcore	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	CPU1 Vcore	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:04	Chassis Intrusi	General Chassis intrusion	Assertion Event
SEL record 02	06/07/2006	10:04:47	Thermal Trip1	State Asserted	Deassertion Event
SEL record 02	06/07/2006	10:04:47	CPU1 Internal E	State Asserted	Assertion Event

① **System Event Log**: Click on this function key to display the System Health Event Log for the remote host system.

d. Alert Settings

Alert Settings Screen

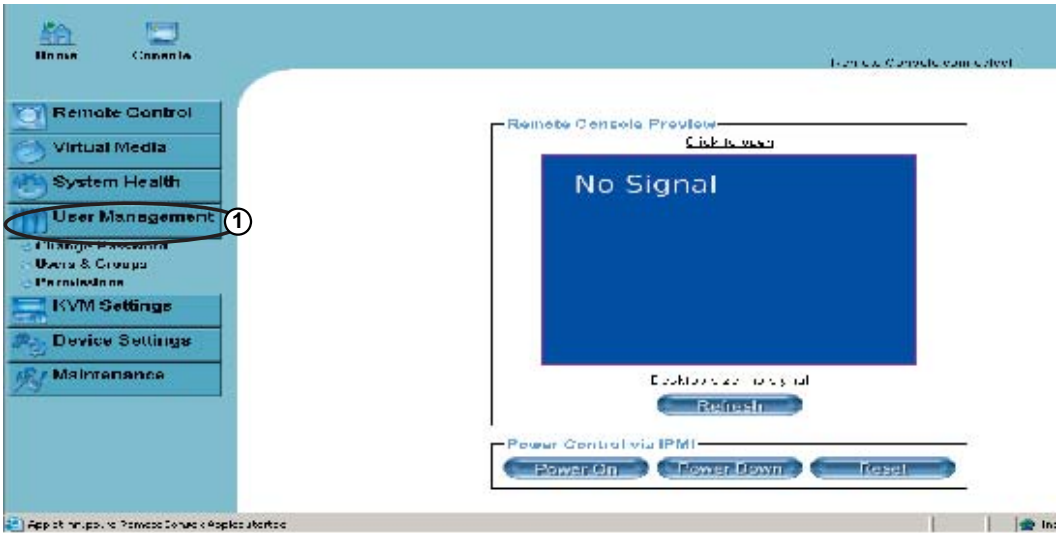

Home
Console
Logout
Remote Control
KVM Console
Remote Power
Virtual Media
Floppy Disk
CD-ROM Image
Drive Redirection
Options
System Health
Chassis Control
Monitor Sensors
System Event Log
Alert Settings
User Management
Change Password
Users & Groups
Permissions
KVM Settings
User Console
Keyboard/Mouse
Device Settings
Network
Dynamic DNS
Security
Certificate
Date/Time
Event Log
SNMP Settings
Maintenance
Device Information
Event Log
Update Firmware
Unit Reset
1
IPMI Alert Configuration
[Filter List]
[Policy List]
[LAN Destination List]
2
3
4
IPMI Filter List
Index Status Filter Type Action Policy# Severity Generator ID Sensor Type Sensor No Trigger Offset Mask Data 1 Data 2 Data 3
1 enabled configurable alert 0 unspecified ff ff ff ff ff ffff ff ff ff ff ff ff ff ff [edit]
2 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
3 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
4 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
5 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
6 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
7 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
8 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
9 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
10 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
11 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
12 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
13 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
14 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
15 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
16 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
17 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
18 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
19 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
20 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
21 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
22 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
23 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
24 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
25 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
26 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
27 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
28 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
29 disabled configurable 0 unspecified 00 00 00 00 00 0000 00 00 00 00 00 00 00 00 [edit]
http://192.168.1.200/home.asp (1 of 2)6/8/2006 4:50:14 PM

① **Alert Settings**: Click on this function key to activate the alert settings submenu for the remote host system. The items monitored include: 1. Filter List, 2. Policy List and 3. LAN Destination List

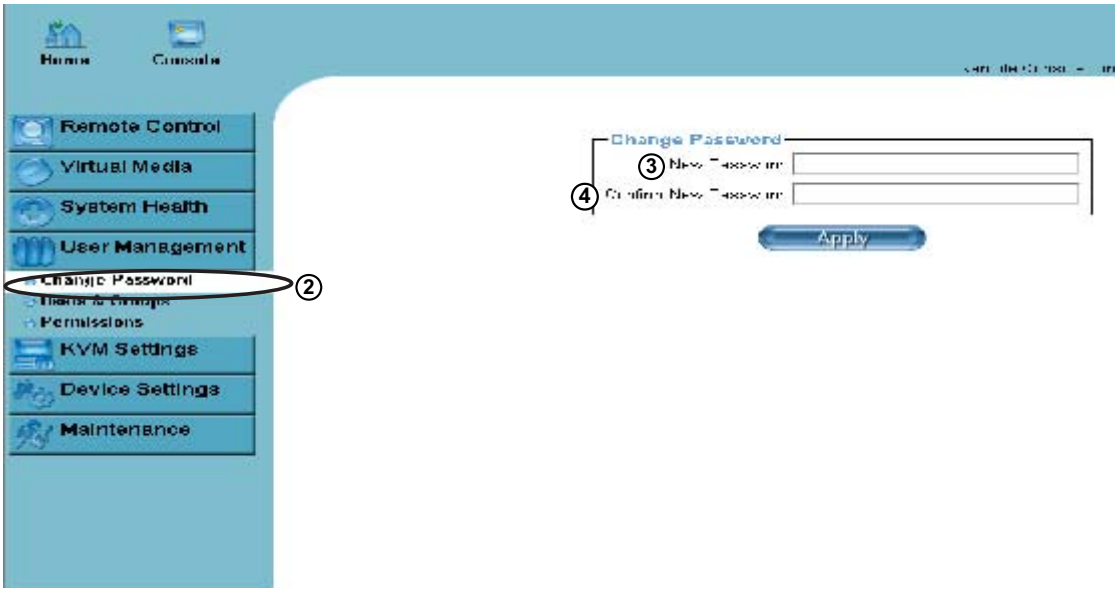
3.2.4. User Management

Click on the User Management icon on the Home Page to activate its submenus: Change Password, Users & Group and Permissions as listed below.

User Management Screen



a. Change Password



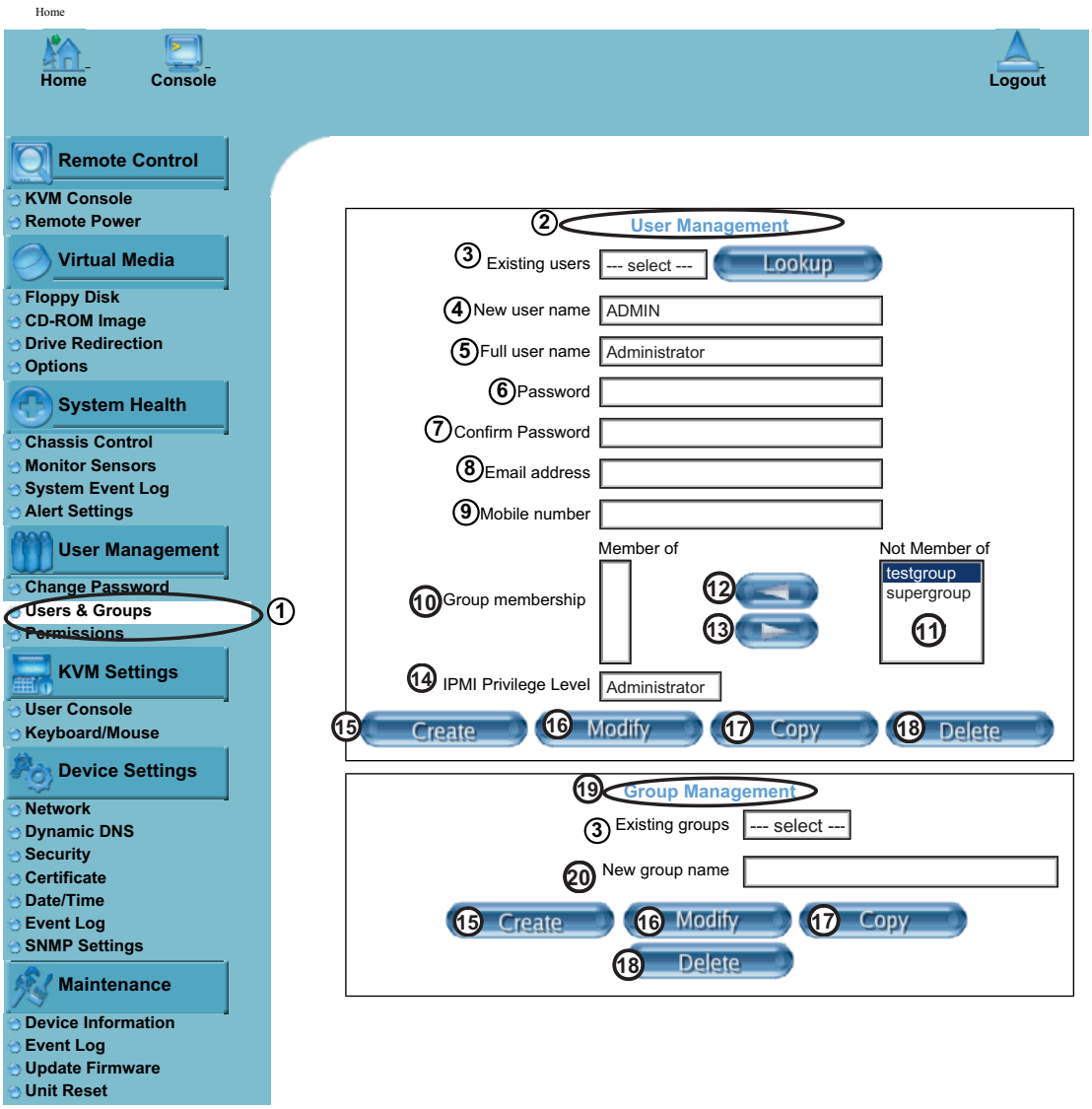
① **User Management:** Click on this icon to activate the User Management submenu. Once this submenu displays, you can access the New Password fields.

② **Change Password:** Click on this function key to access the New Password and Confirm New Password fields.

③ **New Password:** Key in your new password in the blank.

④ **Confirm New Password:** Key in your new password in the blank again and click "Apply" to confirm it.

b. Users & Groups-User Management and Group Management



① **Users & Groups:** Click on this icon to activate the Users & Groups submenu.

② **User Management:** This window displays the user's information.

③ **Existing users:** Select an existing user for information updates. Once a user is selected, click on the "Lookup" icon on right to view user information.

④ **New user name:** Key in new user name in this field.

⑤ **Full user name:** Key in full user name in this field.

⑥ ⑦ **Password and Confirm Password:** Type the user's password in the field and then type the password again in the next field to confirm it. The password must be 4 characters or longer.

⑧ **Email Address:** Key in the user's email address in the field. (*Optional)

⑨ **Mobile Phone:** Key in the user's mobile phone number in the field. (*Optional)

⑩ **Group Membership:** This field indicates the group that the user belongs to. To select a group, click on the group name on the "Not Member Of" window to select it as shown in Window ⑪, then click on the backwards arrow shown on ⑫ to enter the group name in the Group Membership field as shown in ⑩. Reverse the procedure to remove the user from a group.

⑭ **IPMI Privilege Level:** Click on the arrow key on the right to activate the Privilege Selection menu. The IPMI Privilege Level contains five categories: No Access, User, Operator, Administrator and OEM.

⑮ **Create:** Click on this button to enter a new user's or group information in the User/ Group Management fields.

⑯ **Modify:** Click on this button to modify a user's or group information in the User/ Group Management fields.

⑰ **Copy:** Click on this button to copy a user's or group information in the User/Group Management fields.

Copy User

Choose an Existing User from the selection box. Enter a new user name in the field "New User Name." Click on the "Copy" button and a new user with the name you've typed in will be created. The properties of the selected user will be copied to the new user.

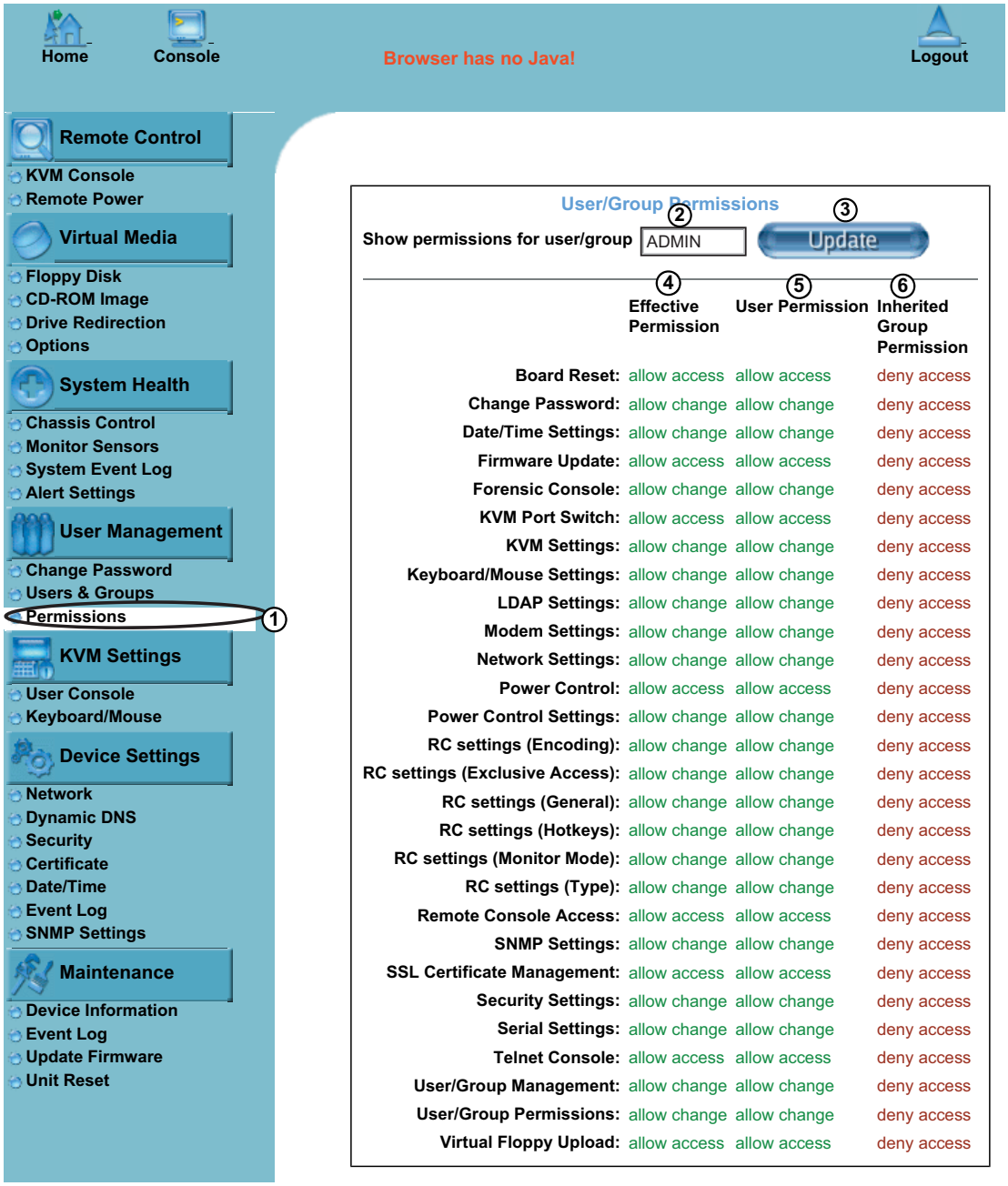
Copy Group

Choose an Existing group from the selection box. Enter a new group name in the field "New Group Name." Click on the "Copy" button and a new group with the name you've typed in will be created. The properties of the selected group will be copied to the new group.

⑱ **Delete:** Click on this button to delete a user's or group information in the User/ Group Management fields.

⑲ **Group Management:** This window allows you to enter group information for better user management.

c. Permissions


Home
Console
Browser has no Java!
Logout
Remote Control
KVM Console
Remote Power
Virtual Media
Floppy Disk
CD-ROM Image
Drive Redirection
Options
System Health
Chassis Control
Monitor Sensors
System Event Log
Alert Settings
User Management
Change Password
Users & Groups
Permissions
KVM Settings
User Console
Keyboard/Mouse
Device Settings
Network
Dynamic DNS
Security
Certificate
Date/Time
Event Log
SNMP Settings
Maintenance
Device Information
Event Log
Update Firmware
Unit Reset
User/Group Permissions
Show permissions for user/group
ADMIN
Update
Effective Permission
User Permission
Inherited Group Permission
Board Reset: allow access allow access deny access
Change Password: allow change allow change deny access
Date/Time Settings: allow change allow change deny access
Firmware Update: allow access allow access deny access
Forensic Console: allow change allow change deny access
KVM Port Switch: allow access allow access deny access
KVM Settings: allow change allow change deny access
Keyboard/Mouse Settings: allow change allow change deny access
LDAP Settings: allow change allow change deny access
Modem Settings: allow change allow change deny access
Network Settings: allow change allow change deny access
Power Control: allow access allow access deny access
Power Control Settings: allow change allow change deny access
RC settings (Encoding): allow change allow change deny access
RC settings (Exclusive Access): allow change allow change deny access
RC settings (General): allow change allow change deny access
RC settings (Hotkeys): allow change allow change deny access
RC settings (Monitor Mode): allow change allow change deny access
RC settings (Type): allow change allow change deny access
Remote Console Access: allow access allow access deny access
SNMP Settings: allow change allow change deny access
SSL Certificate Management: allow access allow access deny access
Security Settings: allow change allow change deny access
Serial Settings: allow change allow change deny access
Telnet Console: allow access allow access deny access
User/Group Management: allow change allow change deny access
User/Group Permissions: allow change allow change deny access
Virtual Floppy Upload: allow access allow access deny access
1
2
3
4
5
6

① **Permissions:** Click on this icon to activate the User/Group Permissions submenu.

② **Show Permissions for User/Group:** click on the arrow on the right to activate the user/group permissions selection menu.

③ **Update:** Click this icon to update permissions information.

④ **Effective Permissions:** This field indicates the actual permissions a user/group has.

⑤ **User Permissions:** This field indicates the actual permissions a user has.

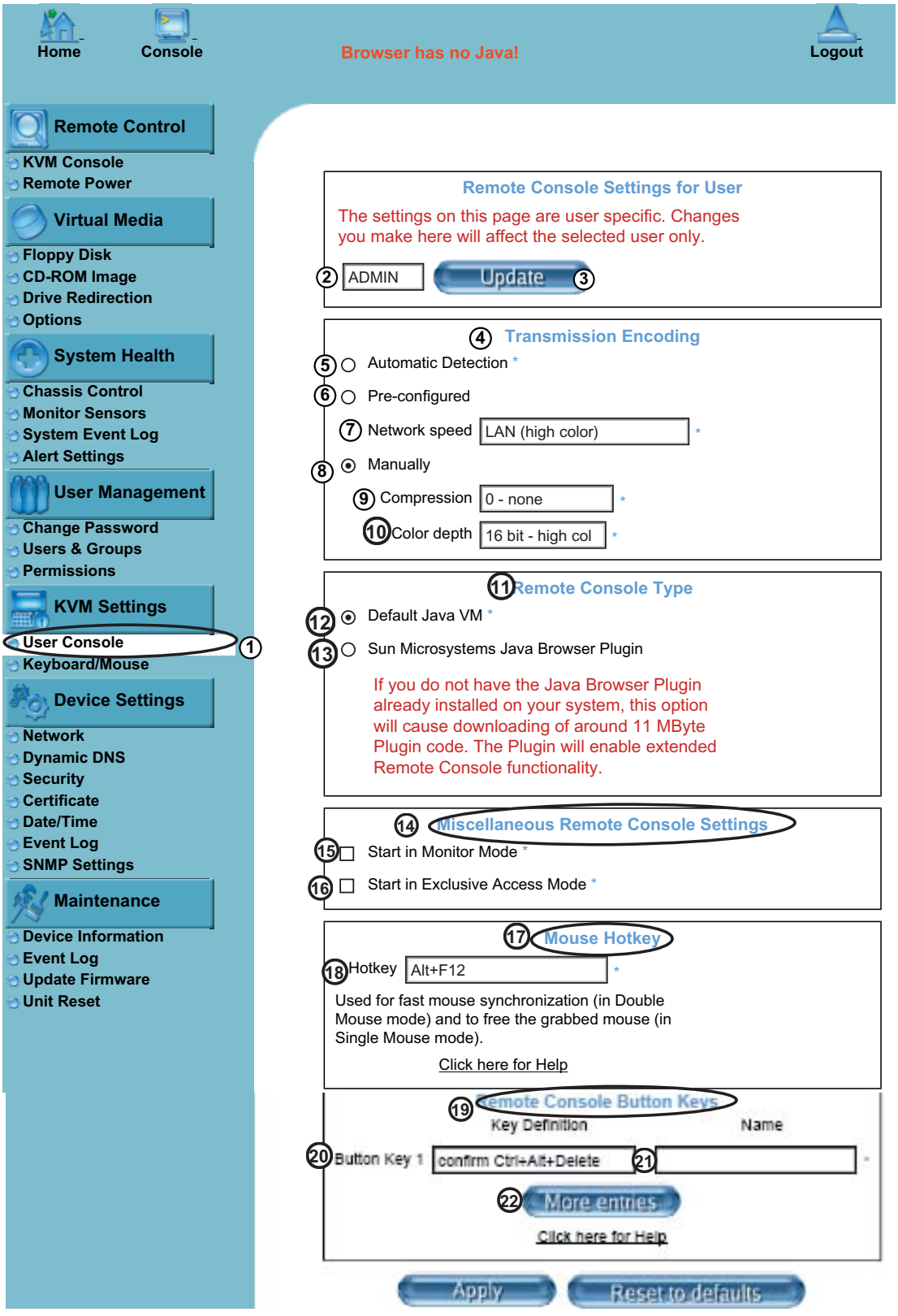
⑥ **Inherited Group Permission:** This field indicates the permissions a user has due to the fact that he or she belongs to a certain group.

3.2.5. KVM Settings

Click on the KVM Settings icon on the Home Page to activate its submenus: User Console and Keyboard/Mouse as listed below.

a. User Console

KVM Settings: User Console



a. User Console

1. User Console: Click on this icon to activate the User Console submenu.

2. User Selection: This field allows you to decide which group the user belongs to. Click on the arrow on the right to activate the selection menu and highlight the name of the group to select it.

3. Update: Once you've selected the group name, click on Update to save the selections.

4. Transmission Encoding: This field allows the user to decide how (the video) data is transmitted between the local system and the remote host.

5. Automatic Detection: Select this option to allow the OS to automatically detect the networking configuration settings such as the bandwidth of the connection line, and transmit data accordingly. (You can only select one item from #5, #6 and #8.)

6. Pre-configured: This item allows the user to select the data transmission setting from a pre-defined options list. The pre-configured settings will provide the best result because the compression and color depth settings will be adjusted for optimization based on the network speed indicated. (You can only select one item from #5, #6 and #8.)

7. Network speed: Once you've selected the pre-configured option above, you then can select a desired network speed setting from the selection menu by clicking on the arrow on the right.

8. Manually: You can select a desired network speed setting from the selection menu by clicking on the arrow on the right. This item allows the user to adjust both compression and color depth settings individually. (You can only select one item from #5, #6 and #8.)

9. Compression: Data signal transmission is compressed to save bandwidth. High compression rates will slow down network interfacing and shall not be used when several users are connected to the network.

10. Color Depth: Click on the arrow on the right to select either 16 bit-high colors or 8 bit-256 colors. The standard color depth is 16 bit-high color. This setting is recommended for compression level 0. For typical desktop interfaces, the setting of 8 bit-256 colors is recommended for faster data transmission.

11. Remote Console Type: This field allows the user to decide which Remote Console Viewer to use.

12. Default Java VM (JVM): Select this option to use the default Java Virtual Machine of your web browser. This can be the Microsoft JVM for Internet Explorer or the Sun JVM depending on the configuration of your browser.

13. Sun Microsystems Java Browser Plugin: Select this option when the JVM used to run the code for the Remote Console is a Java Applet. If you use this function for the first time and the appropriate Java plugin is not yet installed in your system, you may download and install it automatically. To download and install it, you need to check "yes" in the dialogs. Downloading Sun's JVM will allow you to use a stable and identical JVM across different platforms. (*Note: If your internet connection is slow, please pre-install the JVM on your administration machine.)

14. Miscellaneous Remote Console Settings: This window allows you to specify the following Remote Console Settings.

15. Start in Monitor Mode: Check this box to enable the Start in Monitor Mode which will allow data to be displayed in the remote monitor as soon as Remote Console is activated. (The data displayed in the remote monitor is ready-only.)

16. Start in Exclusive Access Mode: Check this box to enable the exclusive access mode immediately at Remote Console startup, which will force all other users connected to the network to close. No other users can open the Remote Console until you disable this function or log off.

17. Mouse Hotkey: This option allows you to use a hotkey combination to specify the mouse synchronization mode or the single mouse mode.

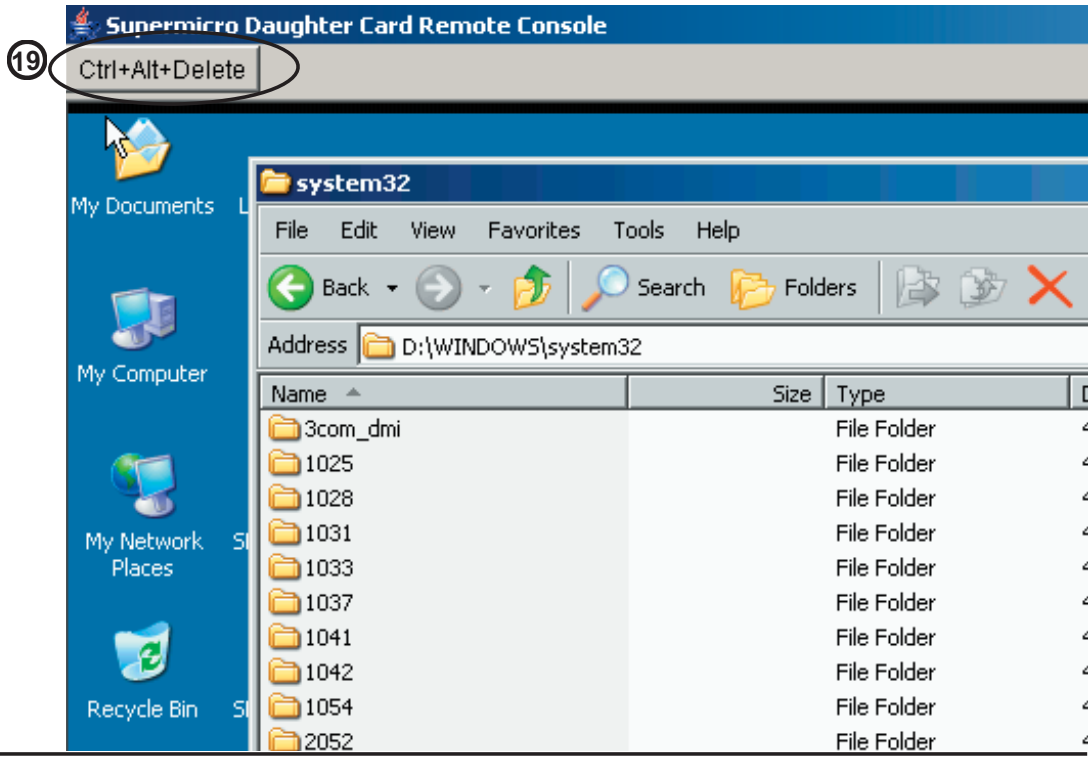
18. Hotkey: Enter a hotkey combination in the box to specify the mouse synchronization mode or the single mouse mode.

19. Remote Console Button Keys: This window allows the user to define button keys for the remote host. The button keys allow simulating keystrokes on a remote host or issuing commands to a remote system. The button keys are needed when you have a missing key or when you want to prevent interference caused to the local system. After a remote console button key is set, it will appear on the right upper corner of the remote monitor screen as shown in the graphics below. (*For details instructions in creating button keys, please click on the link-"Click here for Help.")

20 Button Keys: Enter the syntax of a button key in the box. (*For detailed instructions in creating button keys, please click on the link-"Click here for Help.")

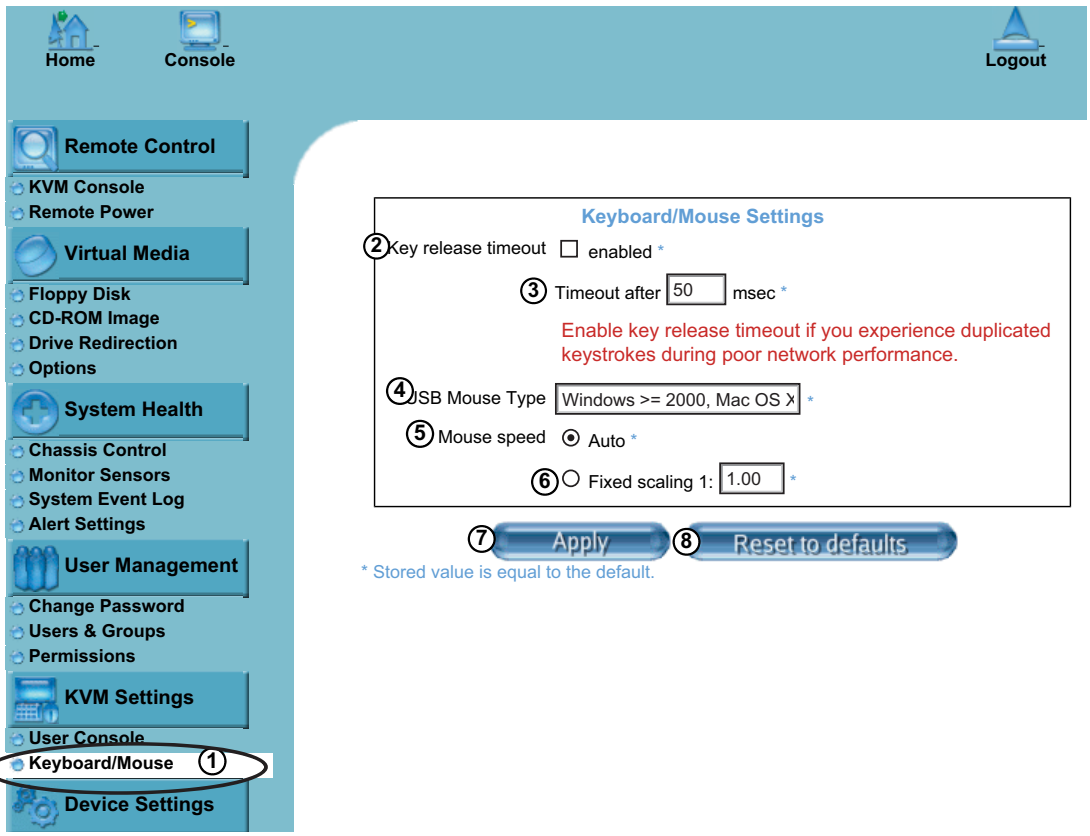
21 Name: Key in the name of a button key in the box. (*For details instructions in creating button keys, please click on the link-"Click here for Help.")

22 More Entries: Click on this icon to create more Button Keys.



b. Keyboard/Mouse

KVM Settings: Keyboard/Mouse



1. Keyboard/Mouse: Click on this function key to configure the following Keyboard/Mouse Settings.

2. Key Release Timeout: Check this box to enable the function of "Key Release Timeout," which will set the time limit for a key to be pressed by the user.

3. Timeout after_____msec: If the "Key Release Timeout" indicated above has been enabled, click on the arrow on the right to activate a selection menu to select the timeout setting for the item above.

4. USB Mouse Type: For the USB Mouse to function properly, please select the correct OS for your system from the selection menu by clicking on the arrow on the right.

5. Mouse Speed-Auto: Check the selection to allow your system to automatically set your mouse speed.

6. Fixed Scaling: You can also check the "Fixed Scaling" box and manually key in your selection.

7. Apply: Click on this icon to enter your selections.

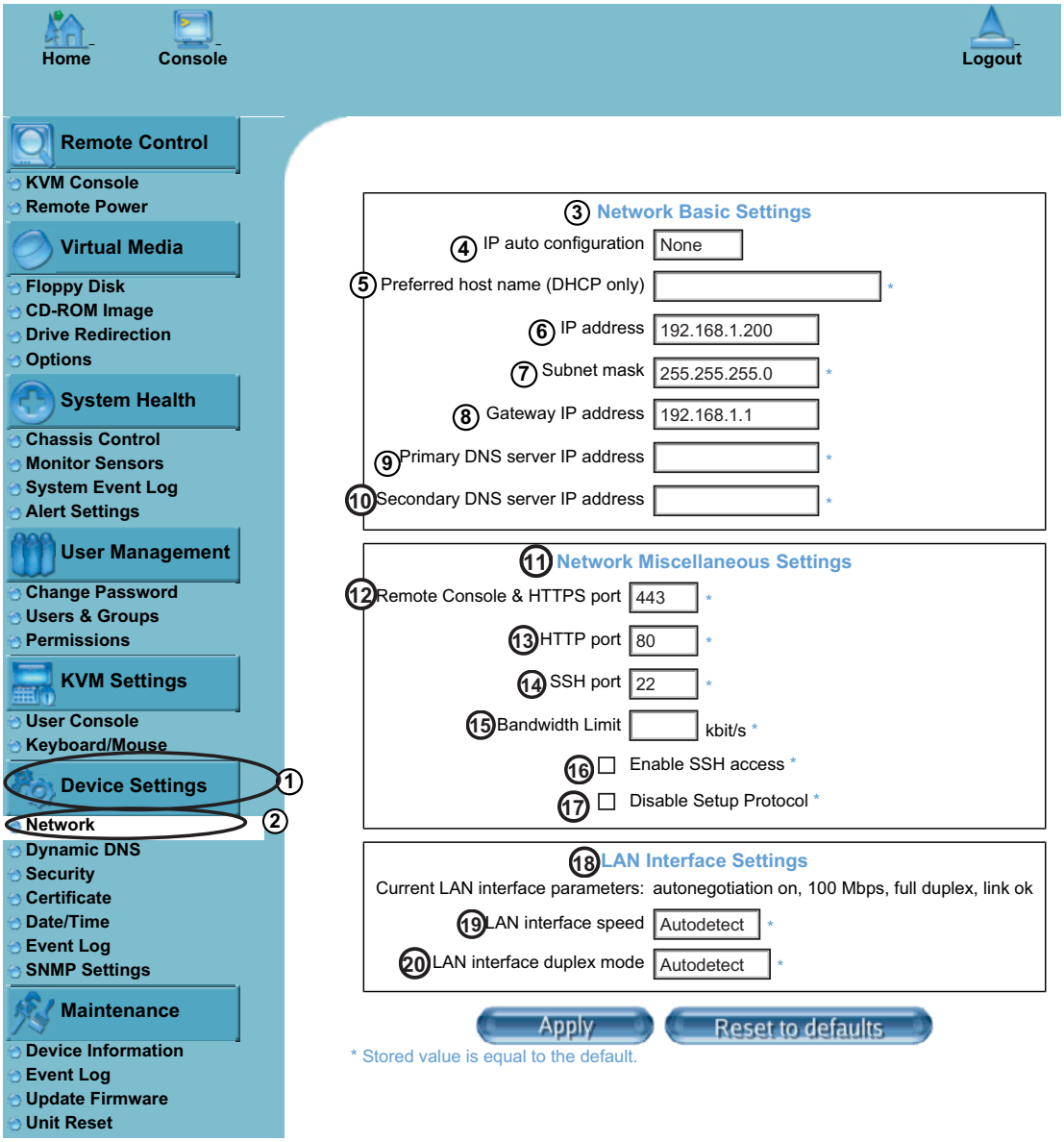
8. Reset to defaults: You can also cancel your selections and use the default values pre-set by the manufacturer by clicking on this icon.

3.2.6. Device Settings

Click on the Device Settings icon on the Home Page to activate its submenus: Network, Dynamic DNS, Security, Certificate, Date/Time, Event Log and SNMP Settings as listed below.

a. Network

Device Settings: Network



a. Network

1. Device Settings: Click on the Device Settings icon to activate its submenus: Network, Dynamic DNS, Security, Certificate, Date/Time, Event Log and SNMP Settings.

2. Network: Click on this function key to activate the Network submenu to configure the following settings: Network Basic Settings, Network Miscellaneous Settings and LAN Interface Settings.

3. Network Basic Settings: This window allows you to configure basic settings for your network.

4. IP Auto Configuration: Click on the box to activate the selection menu and select a desired item from the list. The options are None, DHCP, and BOODP.

5. Preferred Host Name (DHCP only): Enter a Preferred Host Name in the box.

6. IP Address: Enter the IP Address for the remote host in the box.

7. Subnet Mask: Enter the net mask of the local network in the box.

8. Gateway IP Address: Enter the local network router's IP address in this box for the accessibility of the users that are not connected to the local network.

9. Primary DNS Server IP Address: Enter the IP Address of the Primary Domain Name Server in the box.

10. Secondary DNS Server IP Address: Enter the IP Address of the Secondary Domain Name Server in the box. It will be used when the Primary DNS Server cannot be contacted.

11. Network Miscellaneous Setting: This field allows the user to configure the following Network Miscellaneous settings as listed below:

12. Remote Console & HTTPS Port: Enter the port numbers the remote host and the HTTP server are listening. If a number is not entered in the box, the default value will be used.

13. HTTP Port: Enter the port number the HTTP server is listening. If a number is not entered in the box, the default value will be used.

14. SSH Port: Enter the port number the SSH server is listening. If a number is not entered in the box, the default value will be used.

15. Bandwidth Limit: Enter the maximum bandwidth value for network interfacing. The value should be in Kbits per second.

16. Enable SSH Access: Click this box to enable SSH Access.

17. Disable Setup Protocol: Check this box to disable the function of Setup Protocol for the SIMLP card.

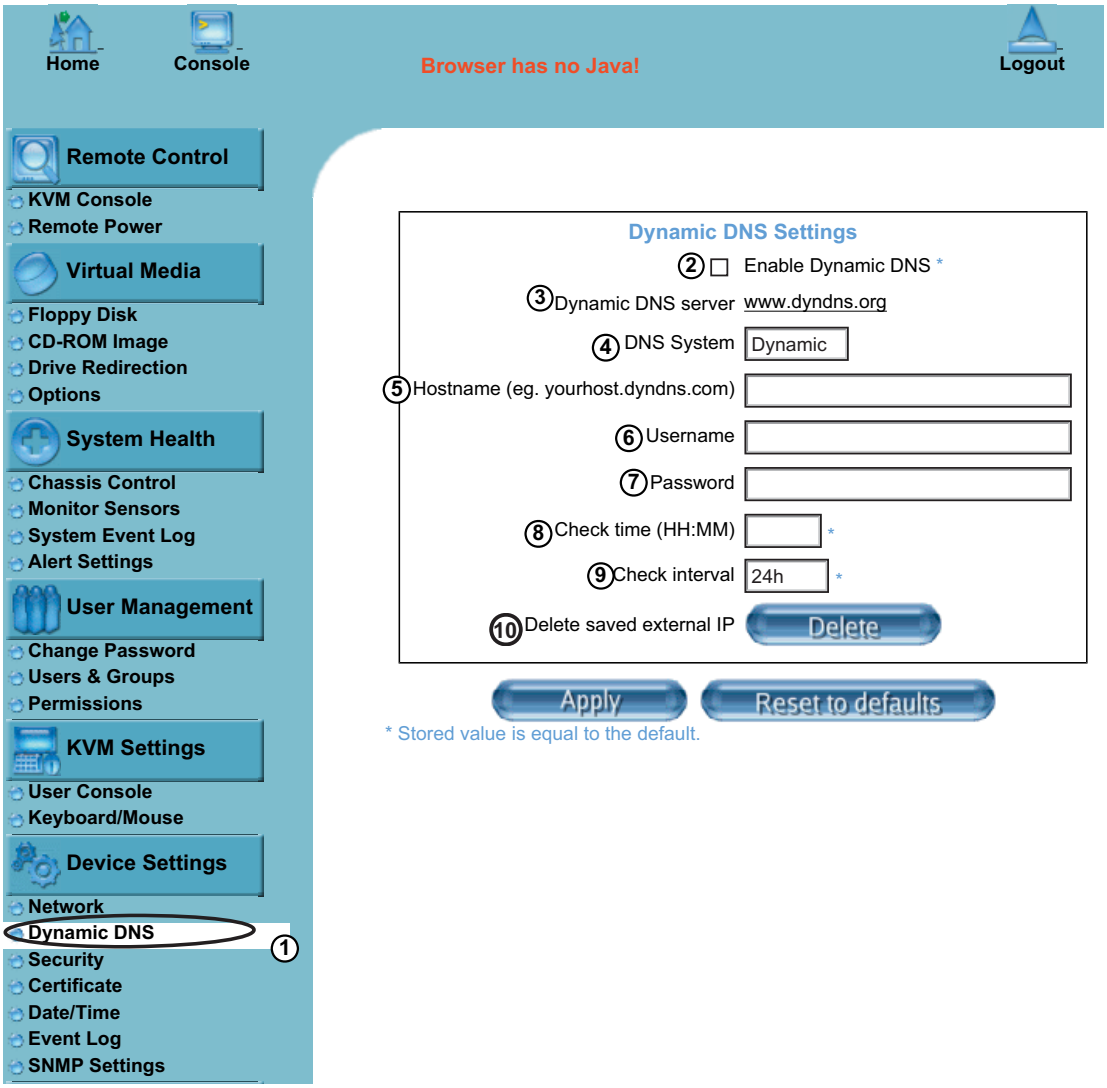
18. LAN Interface Setting: This field allows the user to configure the following LAN Interface settings as listed below:

19. LAN Interface Speed: Click on the arrow on the right to activate the selection menu and select a desired speed. The options are: Auto-detect, 10 Mega bits per second or 100 Mega bits per second. If Auto-detect is selected, LAN Interface Speed will be set at the optimized speed based on the system configurations detected by the OS.

19. LAN Interface Duplex Mode: Click on the arrow on the right to activate the selection menu to select a desired LAN Interface Duplex Mode. The options are: Auto-detect, Half Duplex and Full Duplex. If Auto-detect is selected, the LAN Interface Duplex Mode will be set to the optimized setting based on the system configurations detected by the OS.

b. Dynamic DNS

Device Settings: Dynamic DNS



b. Dynamic DNS

1. Dynamic DNS: Click on this function key to activate its submenu and configure the following Dynamic DNS (-Domain Name Server) settings as listed below.

2. Enable Dynamic DNS: Check this box to enable the Dynamic DNS service.

3. Dynamic DNS Server www.dyndns.org: Click this link to access the DynDNS web site. This is the server name where the DDNS Service is registered.

4. DNS System: Dynamic DNS (Item#2 above) is enabled, you can select from the options: Custom or Dynamic from the selection menu. Select "Custom" to use your own system as the DNS server. Select Dynamic to use the pre-configured Dynamic DNS as your server.

5. Hostname: Enter the name you want to use for the remote host server.

6/7. Username/Password: Enter the username and the password for the remote host user.

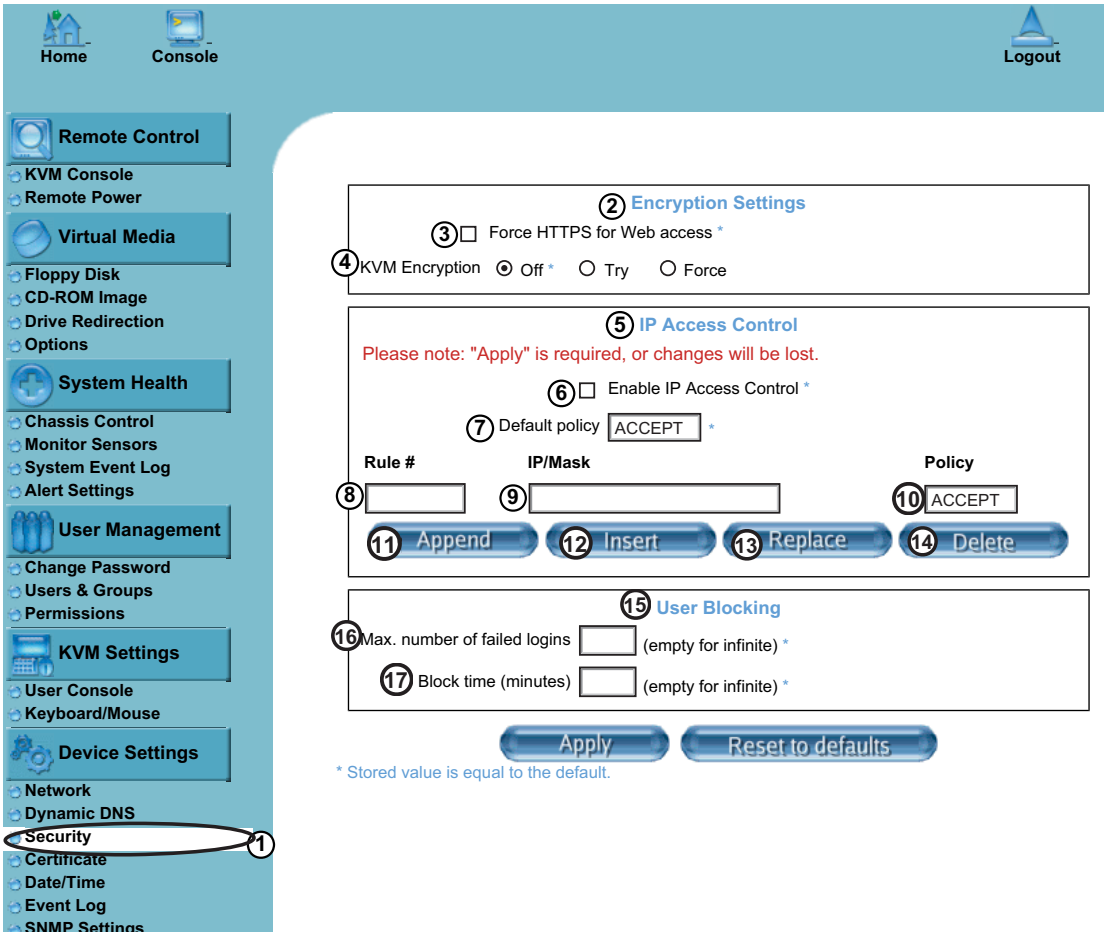
8. Check time (HH:MM): Enter the time the SIMLP card first registers with the DNS server in the HH:MM Format. (e.g. 07:25, 19:30)

9. Check Interval: Enter the interval for the IPMI to report to the Dynamic DNS again.

10. Delete Saved External IP Address: Click on the Delete Icon to delete the IP Address for an external system that has been previous entered and saved.

c. Security

Device Settings: Security



c. Security

1. Security: Click on this function key to activate its submenu and configure the following Security settings as listed below.

2. Encryption Settings: This window allows you to configure encryption settings.

3. Force HTTPS for Web Access: Check this box to enable the function-Force HTTPS for Web Access. If enabled, you will need to use an HTTPS connection to access to the web.

4. KVM Encryption: This option allows you to configure the encryption of the RFB protocol. RFB is used by the remote host to transmit video data displayed in the host monitor to the local administrator machine, and transmit keyboard and mouse data from the local administrator machine back to the remote host.

If set to "Off," no encryption will be used. If set to "Try," the applet (-JVM of the remote host) will attempt to make an encrypted connection. In this case, when a connection cannot be established, an unencrypted connection will be used. If set to "Force," the applet will make an encrypted connection. In this case, an error will be reported if no connection is made.

5. IP Access Control: This section allows you to configure the IP Access Control settings listed below.

6. Enable IP Access Control: Check this box to enable the function of IP Access Control. This function is used to limit user access to the network by identifying them by their IP addresses. (*This function is available to the LAN interface only.)

7. Default Policy: When item#6 (-IP Access Control) set to "enabled," you can select either "accept" or "drop", allowing access or denying access according to pre-defined rules. (***Note**: If this option is set to "drop," and you do not have a set of rules that will accept the internet connection, then the internet connection over LAN is impossible. In this case, you need to change your security settings via modem or by disabling the IP Access Control.)

8. Rule#: Enter a rule number in the box for a command (or commands) that will be used by the IP Access Control.

9. IP/Mask: Enter the IP Address or an IP Address Range for which the command(s) will be applied.

10. Policy: This item instructs the IPMI what to do with the matching packages.

(***Note:** The sequence or the order of the rules is important. The rules are checked in the ascending order until a rule matches. All rules below the matching one will be ignored. The default policy applies if no matching rules are found.)

11. Append: Select this option to add IP Address/Mask, rules or commands to the existing ones.

12. Insert: Select this option to insert IP Address/Mask, rules or commands to the existing ones.

13. Replace: Select this option to replace an old IP Address/Mask, rule or command with a new one.

14. Delete: Select this option to delete (a part of) an existing IP Address/Mask, rule or command.

15. User Blocking: This window allows you to set the conditions how a user is blocked.

16. Max. Number of Failed Logins: Enter the maximum number of failed attempts or failed logins allowed for a user. If the number of failed logins or attempts exceeds this maximum number allowed, the user will be blocked from system.

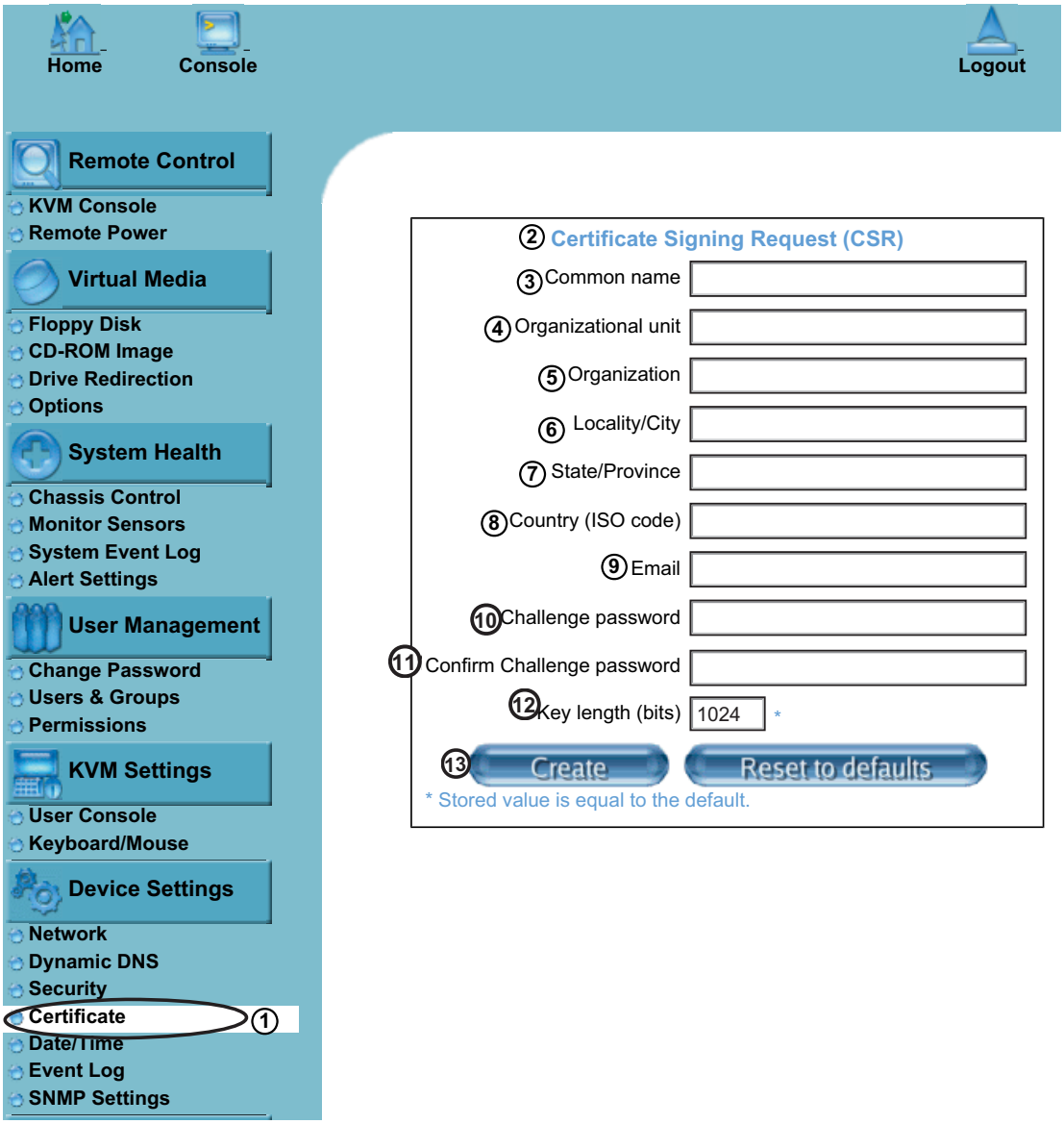
(***Note:** If this box is left empty, the user is allowed to try to login to the server infinitely. For network security, this is not recommended.)

17. Block Time (Minutes): Enter the number of minutes allowed for a user to attempt to login. If the user fails to login within this time allowed, the user will be blocked from system.

(***Note:** If this box is left empty, the user is allowed to try to login to the server infinitely. For network security, this is not recommended.)

d. Certificate

Device Settings: Certificate



d. Certificate

1. Certificate: Click on this function key to activate its submenu and configure the following Certificate settings as listed below.

2. Certificate Signing Request (CSR): This window allows you to define the Certificate Signing Request (CSR) form. The IPMI uses the Secure Socket Layer (SSL) protocol for encrypted network traffic between itself and the remote host servers. When a connection is made, the IPMI has to expose its identity to a remote host by using a cryptographic certificate.

To create a certificate that is unique to a particular IPMI card or SIMLP card, a certification authority (CA) needs to fill out the CSR form indicated in the CSR window above and click "Create" to generate it.

3. Common Name: Enter the (fully qualified domain) network name of the IPMI.

4. Organization Unit: Enter the name of the department within an organation that the IPMI belongs to.

5. Organization: Enter the name of the organization that the IPMI belongs to.

6. Locality/City: Enter the name of the city or the location where the organization is located.

7. State/Province: Enter the name of the state/province where the organization is located.

8. Country (ISO): Enter the name of the country or the ISO code where the organization is located.

9. Email: Enter the email address of a contact person that is responsible for the IPMI.

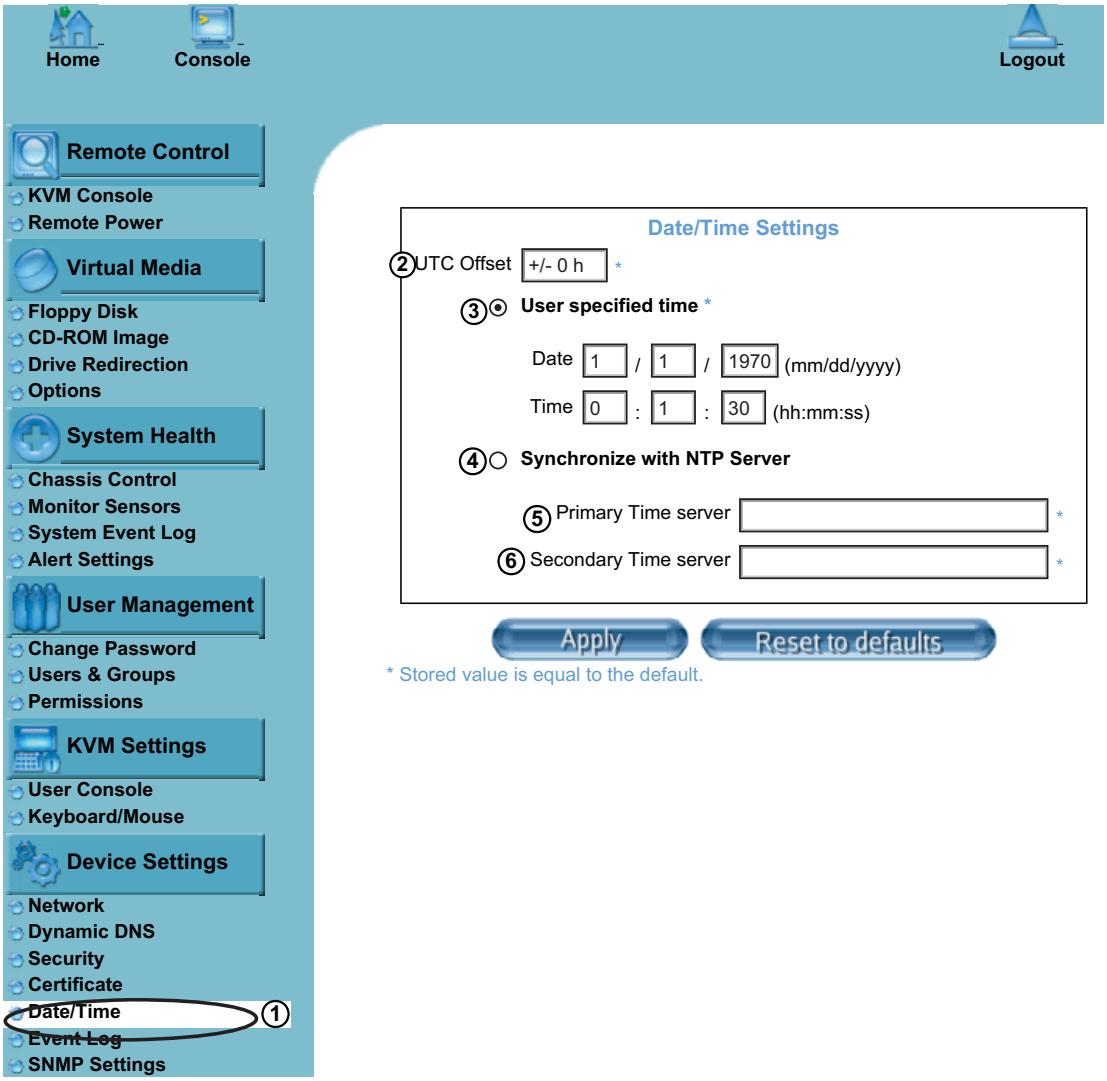
10. Challenge Password: Enter a challenge Password for the Certification Authority to authorize necessary changes to the certificate at a later time. The password shall be four characters or longer.

11. Confirm Challenge Password: Enter a challenge Password one more time to confirm it.

12. Key Length (bits): This is the length of key generated in bits.

e. Date/Time

Device Settings: Date/Time



e. Date/Time

1. Date/Time: Click on this function key to activate its submenu. This feature allows you to set the internal realtime clock for your SIMLP card.

2. UTC Offset: This window allows you to offset the UTC Timer.

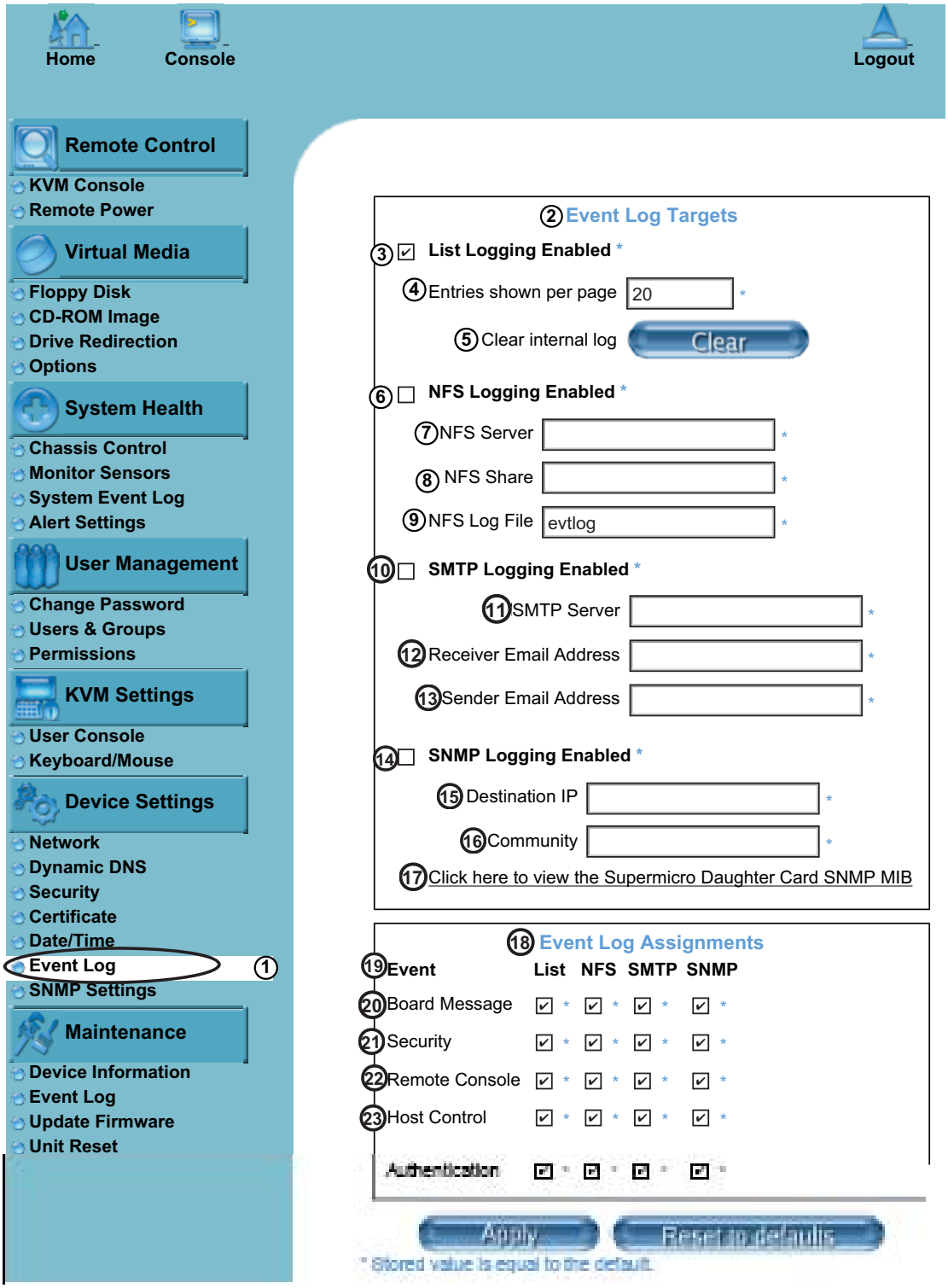
3. User Specified Time: This option allows the user to enter the time values for the SIMLP internal realtime clock.

4. Synchronize with NTP Server: Enter the IP Address for the NTP (Network Time Protocol) Server that you want your SIMLP internal realtime clock to synchronize with.

5/6. Primary Time Server/Secondary Time Server: Enter the IP Address for the primary NTP Server and the secondary NTP Server that you want your SIMLP internal realtime clock to synchronize with. (*The daylight saving time cannot be automatically adjusted. Please manually set up the UTC offset twice a year for your timer to work properly.)

f. Event Log

Device Settings: Event Log



f. Event Log

1. Event Log: Click on this function key to activate its submenu. This feature allows you to set Event Log Targets and Event Log Assignment.

2. Event Log Targets: This section allows you to manually set the event log targets and settings.

3. List Logging Enabled: Check this box to activate the event-logging list. To show the event log list, click on "Event Log" on the "Maintenance" page. (*The maximum number of log list entries is 1,000 events. Every entry that exceeds this limit will automatically override the oldest one in the list. If the reset button is pressed, all logging information will be saved; however, all logging data will be lost if hard reset is performed or the system loses power.)

4. Entries Shown Per Page: Enter the number of entries you want to display on a page.

5. Clear Internal Log: Click this icon to clear internal event log from the memory.

6. NFS Logging Enable: Click this box to enable NFS Logging which will create a Network File System (NFS) for the event logging data to be written into.

7. NFS Server: Enter the IP Address of the NFS Server.

8. NFS Share: Enter the path of the Network File System in which the event logging data is stored.

9. NFS Log File: Enter the filename of the Network File System in which the event logging data is stored.

10. SMTP Logging Enable: Check this box to enable the function of SMTP (Simple Mail Transfer Protocol) logging.

11. SMTP Server: Enter the IP Address for the SMTP Server.

12. Receiver Email Address: Enter the email address that the SMTP event logging data will be sent to.

13. Sender Email Address: Enter the email address from which the SMTP event logging data is sent.

14. SNMP Logging Enable: Check this box to enable the function of SNMP (Simple Network Management Protocol) logging.

15. Destination IP: Enter the IP address where the SNMP trap will be sent to.

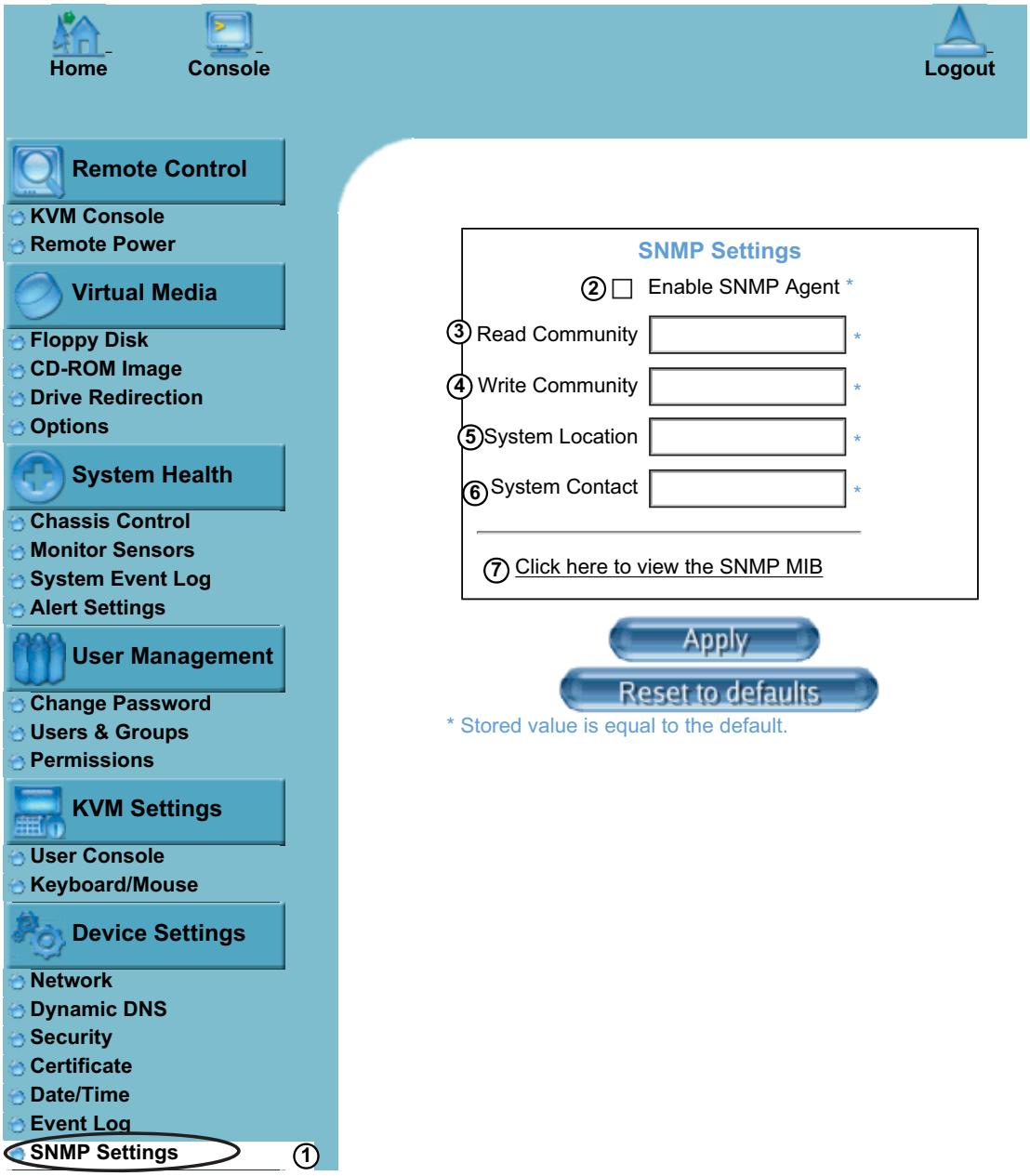
16. Community: Enter the name of the community if the receiver requires a community string.

17. Click here to view the Supermicro Daughter Card SNMP MIB: Click this link to see the SMLP card SNMP MIB.

18. Event Log Assignments: This window allows you to specify the types and the destination for the event logging.

g. SNMP Settings

Device Settings: SNMP Settings



g. SNMP Settings

1. SNMP Settings: Click on this function key to activate its submenu. This feature allows you to configure Simple Network Management Protocol settings.

2. Enable SNMP Agent: Check the box to enable the SNMP Agent and allow it to interface with your SIMLP card.

3. Read Community: Enter the name of the SNMP Community from which you will retrieve information via SNMP.

4. Write Community: Enter the name of the SNMP Community to which you can write information and issue commands via SNMP.

5. System Location: Enter the physical location of the SNMP host server. This location will be used in response to the SNMP request as "sysLocation0."

6. System Contact: Enter the name of the contact person for the SNMP host server. This value will be referred to as "sysContact0."

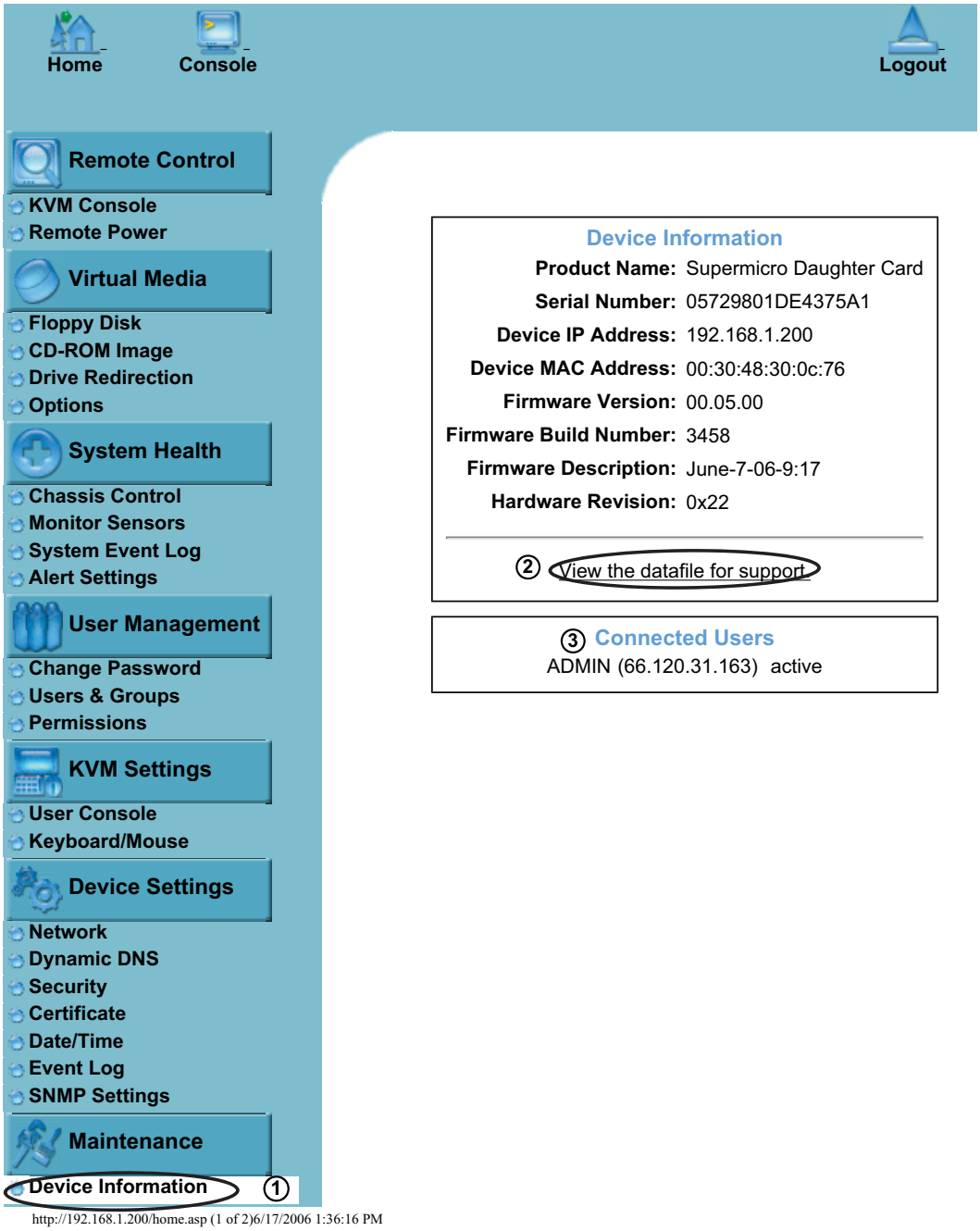
7. Click here to view the SNMP MIB: Click this link to view the SMLP card SNMP MIB file. This file may be necessary for an SNMP client to interface with the SIMLP card.

3.2.7 Maintenance

Click on the Maintenance icon on the Home Page to activate its submenus: Device Information, Event Log, Update Firmware and Unit Reset Settings as listed below.

a. Device Information

Maintenance: Device Information



http://192.168.1.200/home.asp (1 of 2)6/17/2006 1:36:16 PM

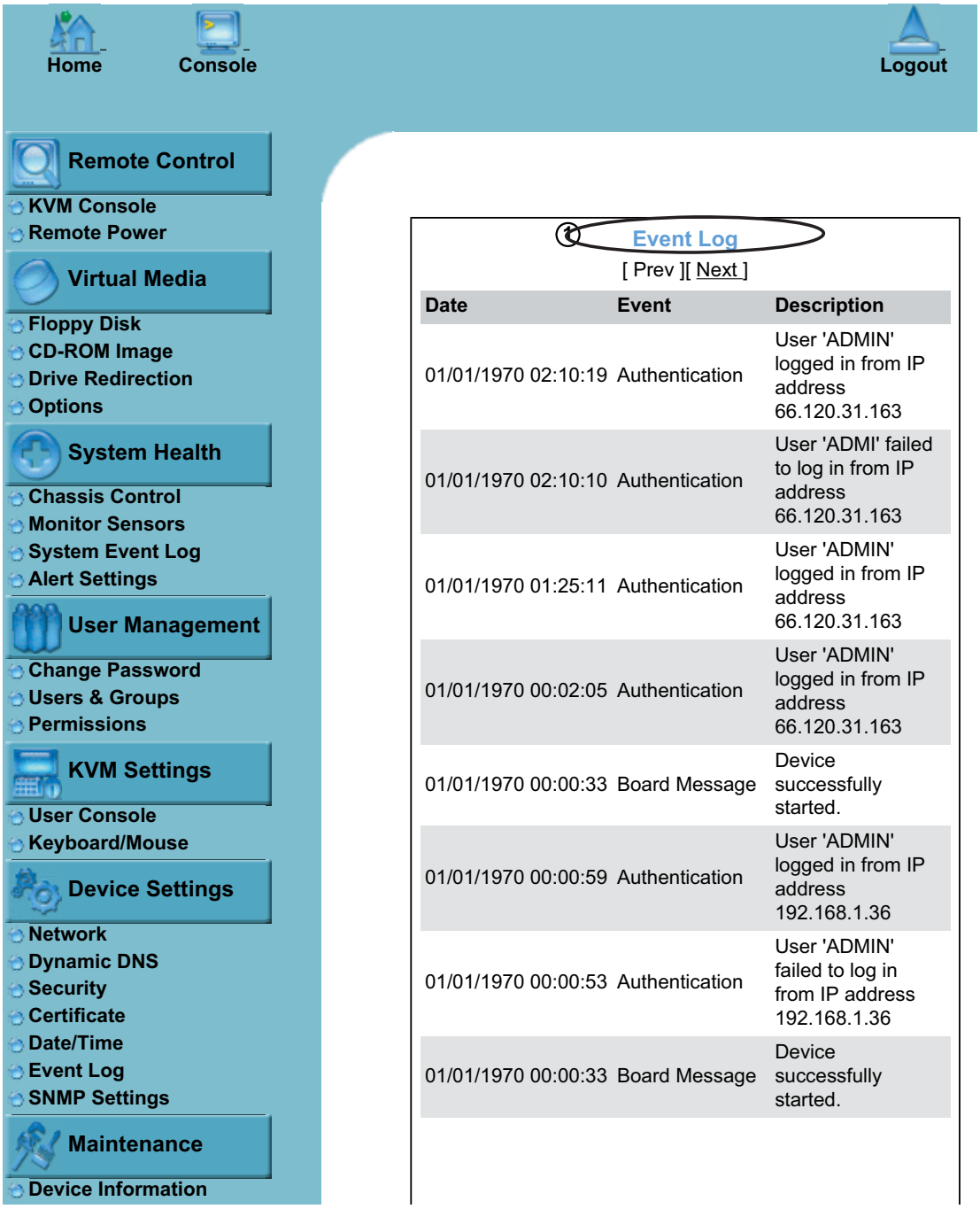
1. Device Information: Click on this function key to activate its submenu. This feature displays the information of the SIMLP card and its firmware.

2. View the Data File for Support: Click on this link to view the XML file which contains you and your product information which is needed for technical support.

2. Connect Users: List the name(s), the IP Address(es) and the status of the connect person(s).

b. Event Log

Maintenance: Event Log

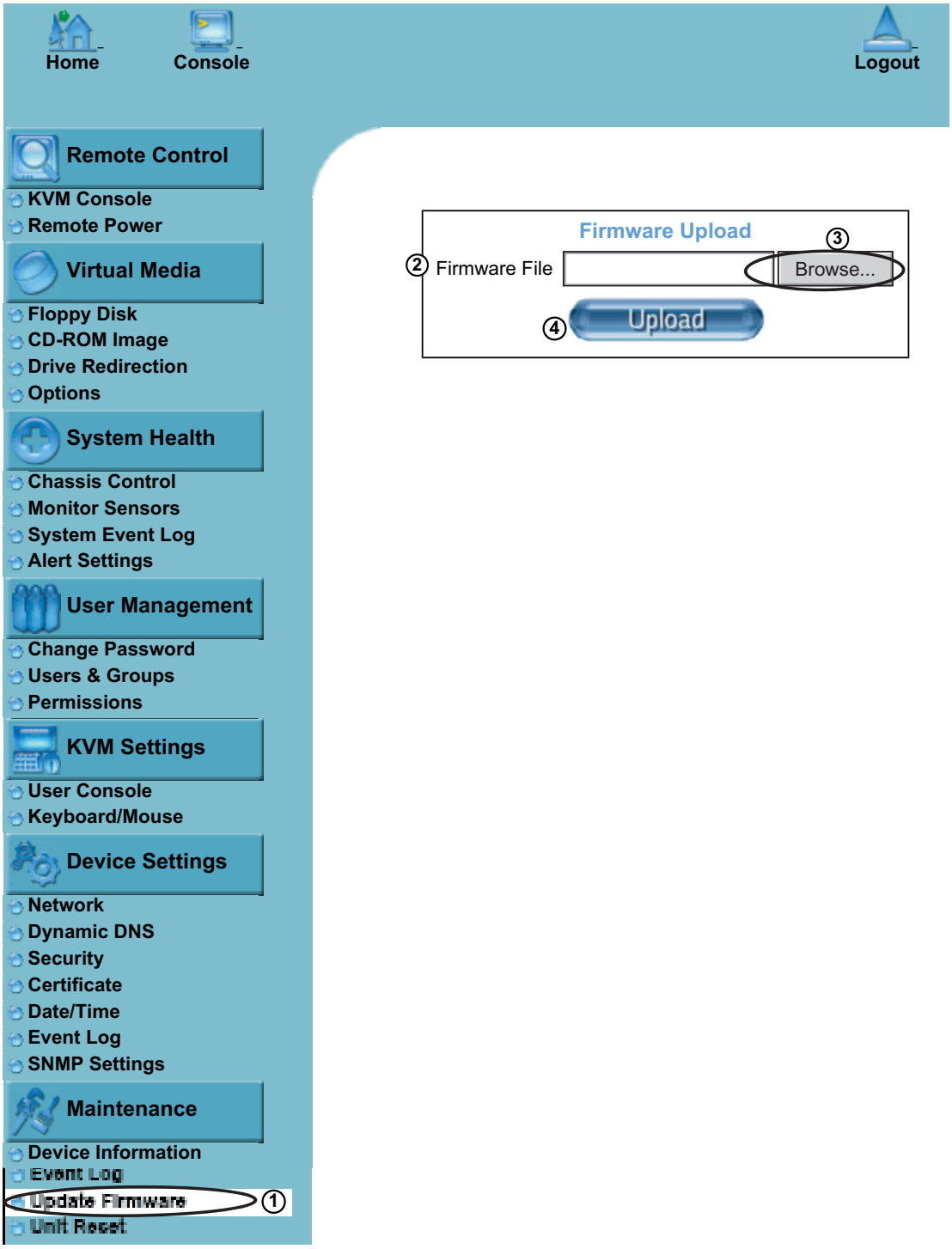


Date	Event	Description
01/01/1970 02:10:19	Authentication	User 'ADMIN' logged in from IP address 66.120.31.163
01/01/1970 02:10:10	Authentication	User 'ADMI' failed to log in from IP address 66.120.31.163
01/01/1970 01:25:11	Authentication	User 'ADMIN' logged in from IP address 66.120.31.163
01/01/1970 00:02:05	Authentication	User 'ADMIN' logged in from IP address 66.120.31.163
01/01/1970 00:00:33	Board Message	Device successfully started.
01/01/1970 00:00:59	Authentication	User 'ADMIN' logged in from IP address 192.168.1.36
01/01/1970 00:00:53	Authentication	User 'ADMIN' failed to log in from IP address 192.168.1.36
01/01/1970 00:00:33	Board Message	Device successfully started.

1. Event Log: Click on the function key on the left to activate the Event Log sub-menu. Once the submenu is displayed, the Event Log List will dispaly. **The Event Log List** contains the information of events that are recorded by the SIMLP in the order of Date/Time, Types, and the descriptions of the events including the IP address(es), person(s) and activities involved .

c. Update Firmware

Maintenance: Update Firmware



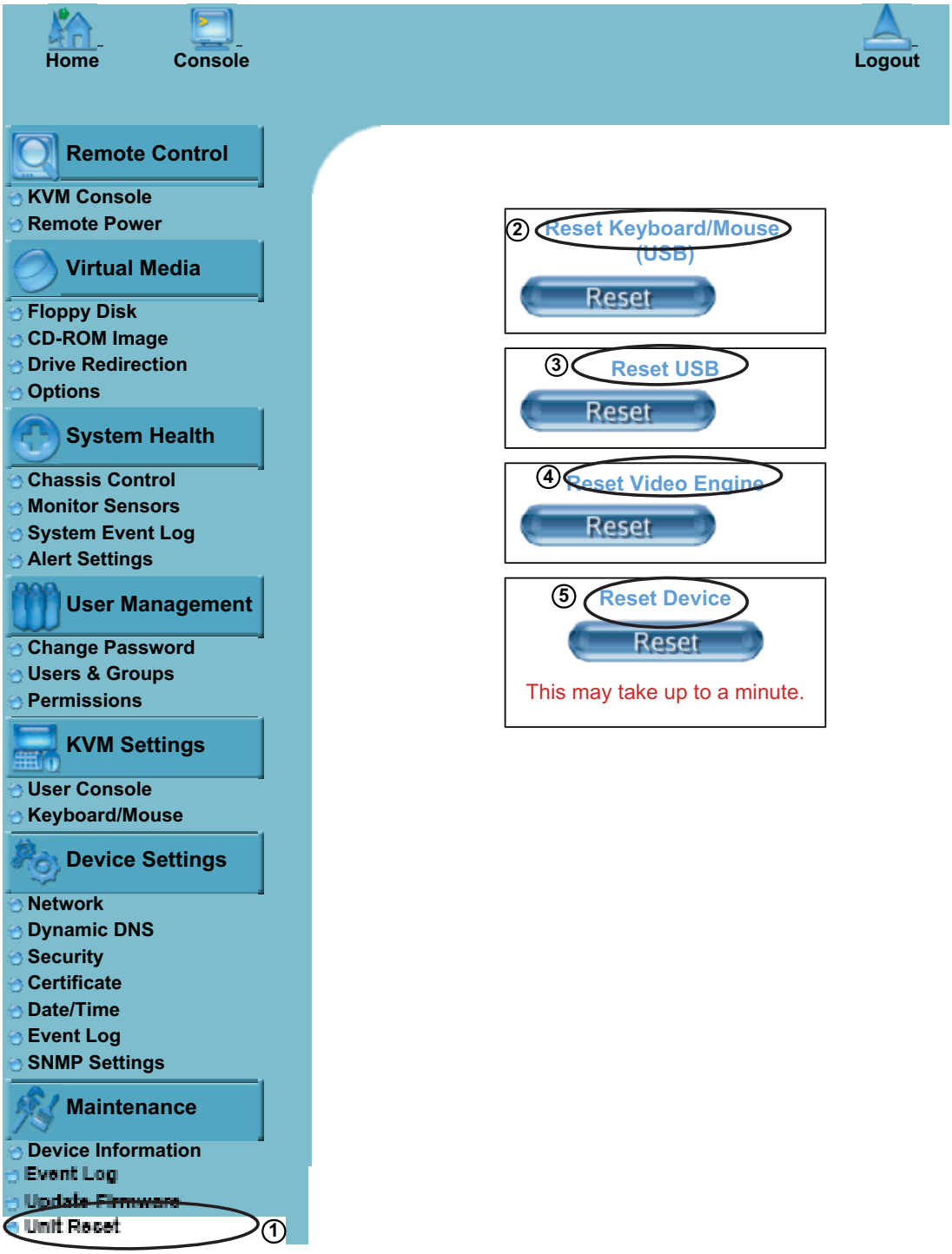
1. Update Firmware: Click on this function key to enable "Update Firmware."

2/3. Firmware File: Enter the name of the firmware you want to update or click on the "Browser" icon to select the firmware file.

4. Update: Click on the "Upload" icon to upload the firmware file to the server for the update. **(*Note**: This process is not reversible once the firmware is updated, so proceed with caution. It might take a few minutes to complete the procedure.)

d. Unit Reset

Maintenance: Unit Reset



1. **Unit Reset:** This feature allows you to reset the following components:
2. **Reset Keyboard/Mouse:** Click the "Reset" icon to reset Keyboard/mouse.
3. **Reset USB:** Click the "Reset" icon to reset the USB module.
4. **Reset Video Engine:** Click the "Reset" icon to reset Video and its controller.
5. **Reset Device:** Click the "Reset" icon to cold reset the IPMI firmware.

Notes